

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/018491

International filing date: 10 December 2004 (10.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-412979
Filing date: 11 December 2003 (11.12.2003)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

13.12.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年12月11日
Date of Application:

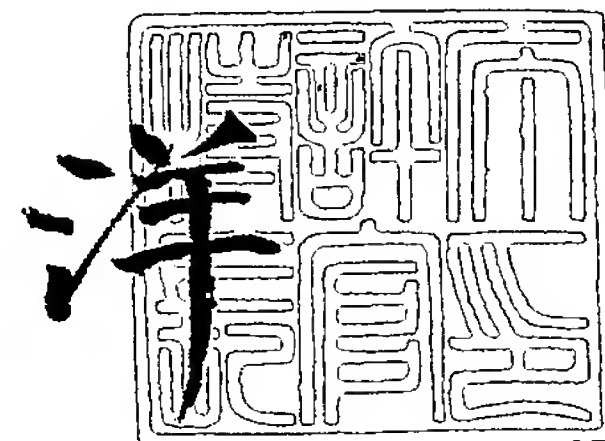
出願番号 特願2003-412979
Application Number:
[ST. 10/C]: [JP2003-412979]

出願人 松下電器産業株式会社
Applicant(s):

2005年 1月27日

特許庁長官
Commissioner,
Japan Patent Office

小川



【書類名】 特許願
【整理番号】 2054051338
【提出日】 平成15年12月11日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/08
H04L 29/06
H04N 5/91
H04J 1/05

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 森岡 芳宏

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 綾木 靖

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 臼木 直司

【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社

【代理人】
【識別番号】 100097445
【弁理士】
【氏名又は名称】 岩橋 文雄

【選任した代理人】
【識別番号】 100103355
【弁理士】
【氏名又は名称】 坂口 智康

【選任した代理人】
【識別番号】 100109667
【弁理士】
【氏名又は名称】 内藤 浩樹

【手数料の表示】
【予納台帳番号】 011305
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

送信手段と受信手段の間でデータの packets 通信を行なう packets 送受信系において、

A V データと非 A V データとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、packets ヘッダー付加手段とを具備する packets 送受信手段において、

前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段とを具備する packets 送信手段。

【請求項 2】

前記暗号化データ生成手段内の前記暗号化手段は暗号化に際して暗号化鍵を使用し、前記送信手段手段と前記受信手段手段が規定の条件を具備していることを検証し認証が行われた後に暗号化鍵が前記送信手段手段と前記受信手段手段で共有され、規定の伝送条件により前記暗号化鍵が更新されることを特徴とする請求項 1 記載の packets 送信手段。

【請求項 3】

前記暗号化データ生成手段内の認証手段において、

前記送信手段手段と前記受信手段手段との間で認証を実行するモードと認証を実行しないモードを持ち、どちらのモードにおいても前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダーを付加することを特徴とする請求項 2 記載の packets 送信手段。

【請求項 4】

前記認証手段において認証を実行するモードは、前記外部より入力される制御情報により決定することを特徴とする請求項 3 記載の packets 送信手段。

【請求項 5】

前記外部より入力される制御情報または認証用の T C P ポート情報は、コンテンツ毎にアクセス位置を指定する U R I、または、Q u e r y により拡張された U R I 情報とにより与えられることを特徴とする請求項 4 記載の packets 送信手段。

【請求項 6】

前記外部より入力される制御情報または認証用の T C P ポート情報は、コンテンツ毎にアクセス位置を指定する U R I で要求されたコンテンツの情報の返信時に与えることを特徴とする請求項 4 記載の packets 送信手段。

【請求項 7】

前記認証手段において認証を実行するモードは、

前記入力 A V データより抽出した制御情報より決定することを特徴とする請求項 3 記載の packets 送信手段。

【請求項 8】

前記認証手段において認証を実行するモードは、

前記外部より入力される制御情報および前記入力 A V データの双方により決定することを特徴とする請求項 3 記載の packets 送信手段。

【請求項 9】

前記 A V データに関するコピー制御情報により前記暗号化情報ヘッダーを付加するかどうかを決定するヘッダー付加制御手段を具備することを特徴とする請求項 3 から 8 記載の packets 送信手段。

【請求項 10】

前記暗号化情報ヘッダーは、

前記 A V データがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合には付加しない、

また、前記 A V データが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合には付加する、

また、前記 A V データが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない、
また、前記 A V データが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する、
ことを特徴とする請求項 9 記載のパケット送信手段。

【請求項 1 1】

前記コピーフリーコンテンツを放送する放送チャネルは、アナログ放送である VHF、UHF、または BS アナログ放送の放送チャネルであることを特徴とする請求項 1 0 記載のパケット送信手段。

【請求項 1 2】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、および E P N フラグ付きコピーフリーのうち少なくとも 1 つのモードを含んでいることを特徴とする請求項 1 0 記載のパケット送信手段。

【請求項 1 3】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルは、デジタル放送である BS デジタル放送、地上波デジタル放送、または CS デジタル放送の放送チャネルであることを特徴とする請求項 1 0 記載のパケット送信手段。

【請求項 1 4】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信装置または受信ユーザであることを認証された場合に行われることを特徴とする請求項 1 3 記載のパケット送信手段。

【請求項 1 5】

前記認証は、日本のデジタル衛星放送の B-CAD カード、または米国の C A T V 放送で 사용되는 POD カードなどのセキュリティモジュールによる認証であることを特徴とする請求項 1 4 記載のパケット送信手段。

【請求項 1 6】

前記暗号化手段は前記暗号化情報ヘッダーを、前記 A V データがフリーコンテンツの場合には付加しない、または、前記 A V コンテンツの意味のあるデータ単位毎に付加することを特徴とする請求項 3 から 8 記載のパケット送信手段。

【請求項 1 7】

A V データと非 A V データとをそれぞれのデータバッファに入力し、前記 2 つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力することを特徴とする請求項 1 から 1 6 記載のパケット送信手段。

【請求項 1 8】

前記優先制御の方法は、前記非 A V データが前記データバッファでオーバーフローしない様に制御しながら、前記 A V データを前記データバッファから優先して出力することを特徴とする請求項 1 7 記載のパケット送信手段。

【請求項 1 9】

前記前記パケットヘッダー付加手段に出力は、あらかじめ決められた間隔値に対して一定のゆらぎ幅を持った概略一定間隔毎に出力する様に、パケットシェーピングして出力することを特徴とする請求項 1 7 記載のパケット送信手段。

【請求項 2 0】

前記暗号化鍵を共有するための認証と鍵交換方式は、D T C P 方式であることを特徴とする請求項 1 から 1 9 記載のパケット送信手段。

【請求項 2 1】

前記暗号化鍵の I D 情報または更新情報として整数値を前記暗号化情報ヘッダーまたはパケットヘッダーに付加することを特徴とする請求項 2 0 記載のパケット送信手段。

【請求項 2 2】

パケットヘッダー付加手段から出力されるパケットを H T T P プロトコルで伝送する場合、H T T P パケットのパケット毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項 2 1 記載のパケット送信手段。

【請求項 2 3】

パケットヘッダー付加手段から出力されるパケットを H T T P プロトコルで伝送する場合、T C P プロトコルが切断して再コネクションを張る毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項 2 1 記載のパケット送信手段。

【請求項 2 4】

前記暗号化モードの変化は T C P プロトコルまたは U D P プロトコルのポート番号の変化で検出して設定することを特徴とする請求項 2 0 記載のパケット送信手段。

【請求項 2 5】

前記暗号化モードの情報をパケット内に持つことを特徴とする請求項 2 0 記載のパケット送信手段。

【請求項 2 6】

前記 A V データのパケット化は、R T P、U D P、I P プロトコルで行うことを特徴とする請求項 1 から 2 5 記載のパケット送信手段。

【請求項 2 7】

前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項 2 6 記載のパケット送信手段。

【請求項 2 8】

前記 A V データのパケット化は、ハードウェアで行うことを特徴とする請求項 2 6 記載のパケット送信手段。

【請求項 2 9】

マルチキャスト伝送の場合、前記暗号化情報ヘッダーを付加したパケットと付加しないパケットの両方を出力することを特徴とする請求項 2 6 記載のパケット送信手段。

【請求項 3 0】

前記 A V データを前記 R T P、U D P、I P プロトコルによる I P パケット化の前に、フォワードエラーコレクション (F E C) による誤り訂正を付加することを特徴とする請求項 2 6 記載のパケット送信手段。

【請求項 3 1】

前記フォワードエラーコレクション (F E C) はリードソロモン方式またはパリティ方式であることを特徴とする請求項 2 6 記載のパケット送信手段。

【請求項 3 2】

前記暗号化情報ヘッダーを付加する場合は、前期 R T P プロトコルにおいて定義されているマーカービット (M ビット) を有効状態にアサートすることを特徴とする請求項 2 6 記載のパケット送信手段。

【請求項 3 3】

前記 A V データのパケット化は、H T T P、T C P、I P プロトコルで行うことを特徴とする請求項 1 から 2 5 記載のパケット送信手段。

【請求項 3 4】

前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項 3 3 記載のパケット送信手段。

【請求項 3 5】

前記認証モードでは前記 H T T P ヘッダーに、認証モード情報を付加することを特徴とする請求項 3 3 記載のパケット送信手段。

【請求項 3 6】

前記 A V データのパケット化は、受信側からの制御により、R T P または H T T P プロトコルで行うことを切替え制御することを特徴とする請求項 2 6 または 3 3 記載のパケット送信手段。

【請求項 3 7】

前記 A V データのパケット化は、受信側の A V データ出力がディスプレイ充てに出力されて蓄積されない場合は R T P が用い、受信側の A V データ出力が記録メディアに蓄積される場合は H T T P を用いる様に、切替え制御することを特徴とする請求項 3 6 記載のパケット送信手段。

【請求項 3 8】

前記 A V データは、S M P T E 2 5 9 M 規格で規定された非圧縮 S D 方式信号、または、S M P T E 2 9 2 M 規格で規定された非圧縮 H D 形式、または、I E C 6 1 8 8 3 規格で規定された I E E E 1 3 9 4 による D V またはデジタル放送の M P E G - T S の伝送ストリーム形式、または、D V B 規格 A 0 1 0 で規定された D V B - A S I による M P E G - T S 形式、または、M P E G - P E S , M P E G - E S 、M P E G 4 、I S O / I E C H . 2 6 4 の内のいずれか一つのデータストリーム形式を含むことを特徴とする請求項 2 6 から 3 7 記載のパケット送信手段。

【請求項 3 9】

前記 A V データを構成するデータブロックにタイムスタンプを付加し、1 つ以上のタイムスタンプ付データブロックをまとめて R T P または H T T P 上にマッピングすることを特徴とする請求項 3 8 記載のパケット送信手段。

【請求項 4 0】

前記 A V データが M P E G - T S の場合、各 T S パケットにタイムスタンプを付加し、複数のタイムスタンプ付 T S パケットをまとめて R T P または H T T P 上にマッピングすることを特徴とする請求項 3 9 記載のパケット送信手段。

【請求項 4 1】

前記各 T S パケットに付加するタイムスタンプのクロックは M P E G のシステムクロック周波数に等しいことを特徴とする請求項 4 0 記載のパケット送信手段。

【請求項 4 2】

前記 T S パケットに付加されたタイムスタンプより、M P E G - T S のネットワーク伝送により P C R に付加した伝送ジッターを除去して、受信側での M P E G システムクロックの再生を行うことを特徴とする請求項 4 1 記載のパケット送信手段。

【請求項 4 3】

N を 2 以上の整数とした場合、U D P プロトコルまたは T C P プロトコルの N 個のポートを用いて、N 個のフォーマットの A V データをそれぞれのポート毎に割り当てて伝送することを特徴とする請求項 3 8 記載のパケット送信手段。

【請求項 4 4】

U D P プロトコルまたは T C P プロトコルの単一のポートを用いて、複数のフォーマットの A V データを多重して伝送することを特徴とする請求項 3 8 記載のパケット送信手段。

【請求項 4 5】

N を 2 以上の整数、また、M を N より大きい整数とした場合、U D P プロトコルまたは T C P プロトコルの M 個のポートを用いて、N 個のフォーマットの A V データを単一または多重して M 個のポートに割り当てて伝送することを特徴とする請求項 3 8 記載のパケット送信手段。

【請求項 4 6】

複数の A V データを同時に伝送する場合、高データレートの A V データは U D P プロトコルで伝送し、低データレートの A V データは T C P プロトコルで伝送することを特徴とする請求項 3 8 記載のパケット送信手段。

【請求項 4 7】

複数の A V データを同時に伝送する場合、高データレートの A V データより、低データレートの A V データを優先して伝送することを特徴とする請求項 3 8 記載のパケット送信手段。

【請求項 4 8】

前記 A V データの伝送範囲を制限することを特徴とする請求項 2 6 から 3 7 記載のパケッ

ト送信手段。

【請求項 4 9】

前記 A V データの伝送範囲を制限は、I P プロトコルの T T L (T i m e t o L i v e) の値を用いて制限することを特徴とする請求項 4 8 記載のパケット送信手段。

【請求項 5 0】

前期前記 A V データの伝送範囲を制限は、I P パケットの R T T (R o u n d T r i p T i m e) の値を用いて制限することを特徴とする請求項 4 8 記載のパケット送信手段。

【請求項 5 1】

前記 A V データの伝送範囲を制限は、M A C 層のヘッダー情報により制限することを特徴とする請求項 4 8 記載のパケット送信手段。

【請求項 5 2】

前記 I P パケットのパケットサイズは前期送信手段と受信手段の間の I P ネットワークのパス M T U サイズ以下に設定することを特徴とする請求項 2 6 から 3 7 記載のパケット送信手段。

【請求項 5 3】

前記 I P パケットの伝送は、I E E E 8 0 2 . 3 で規定された伝送方法により行われることを特徴とする請求項 2 6 から 3 7 記載のパケット送信手段。

【請求項 5 4】

前記 I P パケットの伝送は、I E E E 8 0 2 . 1 1 で規定された伝送方法により行われることを特徴とする請求項 2 6 から 3 7 記載のパケット送信手段。

【請求項 5 5】

前記 I E E E 8 0 2 . 1 1 の使用において、W E P または W P A またはその他のネットワーク接続制限手段を用いることを特徴とする請求項 5 4 記載のパケット送信手段。

【請求項 5 6】

前記 I P パケットの伝送は、I E E E 8 0 2 . 1 Q により規定された伝送方法により行われることを特徴とする請求項 2 6 から 3 7 記載のパケット送信手段。

【請求項 5 7】

前記 I P パケットの伝送は、I P バージョン 4、または、I P バージョン 6 を使用して行われることを特徴とする請求項 2 6 から 3 7 記載のパケット送信手段。

【請求項 5 8】

前記 I P バージョン 4 を用いる場合、T O S フィールドを用いて優先制御を行なうことを特徴とする請求項 5 7 記載のパケット送信手段。

【請求項 5 9】

前記 I P バージョン 6 を用いる場合、P r i o r i t y フィールドを用いて優先制御を行なうことを特徴とする請求項 5 7 記載のパケット送信手段。

【書類名】 明細書

【発明の名称】 パケット送信手段

【技術分野】

【0 0 0 1】

本発明は、IEEE 802.3などのイーサネット(R) (有線LAN) やIEEE 802.11などの無線LANなどを用いて、暗号化されたAVストリームをIPパケット化して高品質に送信するパケット送信装置に関する。

【背景技術】

【0 0 0 2】

従来、一般家庭において、IEEE 1394を用いて、IEC 61883-4で規定された方式に基づきMP EG-T S信号の暗号化伝送が行なわれている。MP EG-T SなどAVデータを暗号化して伝送する方式の一例として、DTCP (Digital Transmission Content Protection) 方式が規定されている。DTCPは、IEEE 1394やUSBなどの伝送メディア上のコンテンツ保護技術である。DTCP方式は、DTLA (Digital Transmission Licencing Administrator) で規格化された方式であり、HYPERLINK "http://www.dtcp.com" http://www.dtcp.com、HYPERLINK "http://www.dtcp.com/data/dtcp#tut.pdf" http://www.dtcp.com/data/dtcp#tut.pdf、

HYPERLINK "http://www.dtcp.com/data/wp#spec.pdf" http://www.dtcp.com/data/wp#spec.pdfや、書籍「IEEE 1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」、133~149ページで説明されている。

【0 0 0 3】

図21は、DTCP方式を用いたMP EG-T SのIEEE 1394での伝送の一例である。DTCP方式では、送信側をソース(2101)、受信側をシンク(2102)と呼び、暗号化したMP EG-T Sなどのコンテンツをソース(2101)からネットワーク(2103)を介して、シンク(2102)へ伝送している。図18に、補足情報として、ソース機器およびシンク機器の例を併記する。

【0 0 0 4】

次に、図22を用いて、DTCP方式における従来のパケット通信手段の概略を説明する。図22は図21のソース(2101)、およびシンク(2102)の構成の概略図である。まず、DTCP方式に準拠した認証と鍵交換(Authentication and Key Exchange、AKEと略する)が行なわれる。AKE手段(2201)に対して、その認証と鍵交換設定情報が入力され、この情報がパケット化手段(2202)により規定のヘッダーを付加されパケット化され、ネットワーク(2207)に出力される。ここで、パケット化手段(2202)は送信条件設定手段(2203)により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワーク(2207)より入力する信号がパケット受信手段(2204)でパケットヘッダーなどの識別によりフィルタリングされ、AKE手段(2201)に入力される。これにより送信側(ソース)のAKE手段と、受信側(シンク)のAKE手段がネットワーク(2103、2207)を介してお互いにメッセージの通信ができる。すなわち、DTCP方式の手順に従い、認証と鍵交換を実行する。

【0 0 0 5】

送信側(ソース)と、受信側(シンク)で認証と鍵交換が成立すれば、次に、AVデータの伝送を行なう。ソースでは、MP EG-T S信号を暗号化手段(2205)に入力して、MP EG-T S信号を暗号化した後、この暗号化されたMP EG-T S信号をパケット化手段(2202)に入力し、ネットワーク(2207)に出力する。シンクでは、ネットワーク(2207)より入力する信号がパケット受信手段(2204)でパケットヘッダーなどの識別によりフィルタリングされ、復号手段(2206)に入力され、復号されMP EG-T S信号が出力される。

【0 0 0 6】

次に、図22を用い上記手順を補足説明する。図23において、ソースとシンク間はI

IEEE 1394 で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクは D T C P 所定の処理により認証鍵の共有を図る。そして、ソースは認証鍵を用いて交換鍵を暗号化してシンクに送り、シンクで交換鍵が復号される。ソースでは暗号鍵を時間的に変化させるために、時間的に変化するシード情報を生成し、シンクに送信する。ソースでは、交換鍵とシード情報より暗号化鍵を生成して、M P E G - T S をこの暗号化鍵を用いて暗号化手段で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化された M P E G - T S 信号を復号する。

【0007】

図 2 1 は、図 1 8 において M P E G - T S 信号を伝送する場合の IEEE 1394 アイソクロナスパケットの一例である。このパケットは、4 バイト (32 ビット) のヘッダー、4 バイト (32 ビット) のヘッダー C R C、224 バイトのデータフィールド、4 バイト (32 ビット) のトレイラによって構成されている。暗号化されて伝送されるのは 224 バイトのデータフィールドを構成する C I P ヘッダーと T S 信号のうち、T S 信号のみで、他のデータは暗号化されない。ここで、D T C P 方式固有の情報は、コピー保護情報である 2 ビットの E M I (Encryption Mode Indicator)、およびシード情報の L S B ビットである O / E (Odd/Even) であり、これらは上記 32 ビットのヘッダー内に存在するため暗号化されずに伝送される。

【特許文献 1】特開 2 0 0 0 - 5 9 4 6 3 号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、上記従来の構成では以下のような問題点を有していた。従来の D T C P 方式は IEEE 1394 において、アイソクロナスパケットを用いて伝送するため M P E G - T S 信号のリアルタイム伝送ができるが、インターネットの標準プロトコルである I P プロトコルを用いて、イーサネット (R) (IEEE 802.3)、無線 LAN (IEEE 802.11) や、その他の I P パケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。すなわち、I P プロトコルを介して論理的に接続された送信機器と受信機器の間を、暗号化によりコンテンツの機密性や著作権の保護を行なった状態で M P E G - T S 信号など A V ストリームを伝送できないという大きな問題点がある。

【課題を解決するための手段】

【0009】

上記課題を解決するために、本願第 1 の発明は、A V データと非 A V データとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段とを具備する。これにより、M P E G - T S 信号などの A V ストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加することを決めることにより、送受信機器間での信号の互換性を確保しながら、A V ストリームの秘匿性を保つことが可能となる。

本願第 2 の発明は、第 1 の発明における認証手段において、認証を実行するモードは、外部より入力される制御情報により決定する。たとえば、外部より入力される制御情報として、コンテンツ毎にアクセス位置を指定する U R I を与え、その U R I の形式により認証

モードを決定する。たとえば、URIがQueryにより拡張されている場合は、認証が必要であり、そのQuery情報より認証用のTCPポート番号を与えることが可能となる。これにより、認証実行モードを、外部より入力される制御情報により決定することが可能となる。

本願第3の発明は、第1の発明における暗号化データ生成手段において、外部から与えられる規定の送信条件としてそのAVストリームのコピー制御情報(CCI)に従うことを特徴とし、暗号化モードと暗号化情報ヘッダー付加を決定する。これにより、MP EG-T S信号などのAVストリームをそのコピー制御情報に従い暗号化モードを決め、暗号化情報ヘッダーを付加した後、パケット化して伝送するので、AVコンテンツの著作権者が設定したコピー制御モードを継承してパケットの伝送がなされる。すなわち、一定規則による処理を行うため、AVコンテンツの著作権保護を図りつつ、送受信機器間での信号の互換性を確保することが可能となる。

本願第4の発明は、第1の発明において、AVデータと非AVデータとをそれぞれのデータバッファに入力し、2つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力する。たとえば、非AVデータがそのデータバッファでオーバーフローしない様に制御しながら、AVデータをそのデータバッファから優先して出力する。これにより、AVデータと非AVデータの内、重要性の高いデータを優先して送信することが可能となる。

本願第5の発明は、第1の発明において、AVデータを構成するデータブロックにタイムスタンプを付加し、1つ以上のタイムスタンプ付データブロックをまとめてRTPパケットのペイロード部またはH T T Pパケットのペイロード部にマッピングする。たとえば、AVデータがMP EG-T Sの場合、各T Sパケットにタイムスタンプを付加し、複数のタイムスタンプ付T SパケットをまとめてRTPまたはH T T P上にマッピングする。たとえば、各T Sパケットに付加するタイムスタンプのクロックはMP EGのシステムクロック周波数を用いることができる。T Sパケットに付加されたタイムスタンプより、MP EG-T Sのネットワーク伝送によりP C Rに付加した伝送ジッターを除去して、受信側でのMP EGシステムクロックの再生を行うことが可能となる。

本願第6の発明は、第1の発明において、AVデータのパケット化は、受信側からの制御により、RTPまたはH T T Pプロトコルで行うことを切替え制御すること。たとえば、AVデータのパケット化は、受信側のAVデータ出力がディスプレイ充てに出力される場合は遅延の小さいRTPプロトコルを用い、受信側のAVデータ出力が記録メディアに蓄積される場合は再送によりパケット落ちを低減するH T T Pプロトコルを用いる。この様に、切替え制御することにより受信側でディスプレイに出力する場合は低遅延でのAVコンテンツの伝送が可能となり、また、受信側で蓄積する場合はパケットロスによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。

【発明の効果】

【0010】

本願第1の発明によれば、以下のような効果を有する。すなわち、外部から与えられる一定規則によりAVコンテンツの送信の暗号化モードを決めることができる。さらに、暗号化情報ヘッダーを付加ルールを決めることができるため、送受信機器間でのAVストリームの秘匿性を保ちながら信号の互換性を確保することが可能となる。

本願第2の発明によれば、第1の発明における認証手段において、認証実行モードを外部入力の制御情報より決定する。たとえば、外部より入力される制御情報として、コンテンツ毎にアクセス位置を指定するURI (Uniform Resource Identifier) を与え、そのURIの形式により認証モードを決定することができる。一例として、URIがQuery形式により拡張されている場合には認証が必要という情報と

、同時に、その Q u e r y 情報より認証用の T C P ポート番号の情報を与えることが可能となる。これにより、認証実行モードを、外部より入力される制御情報により決定することが可能となる。

本願第 3 の発明によれば、第 1 の発明における暗号化データ生成手段において、外部から与えられる規定の送信条件としてその A V ストリームのコピー制御情報に従うことを特徴とし、暗号化モードと暗号化情報ヘッダー付加を決定する。これにより、M P E G - T S 信号などの A V ストリームをそのコピー制御情報に従い暗号化モードを決め、暗号化情報ヘッダーを付加した後、パケット化して伝送するので、A V コンテンツの著作権者が設定したコピー制御モードを継承してパケットの伝送がなされる。すなわち、一定規則による処理を行うため、A V コンテンツの著作権保護を図りつつ、送受信機器間での信号の互換性を確保することが可能となる。

本願第 4 の発明によれば、第 1 の発明において、A V データと非 A V データとをそれぞれのデータバッファに入力し、2 つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力する。たとえば、非 A V データがそのデータバッファでオーバーフローしない様に制御しながら、A V データをそのデータバッファから優先して出力する。これにより、A V データと非 A V データの内、重要性の高いデータを優先して送信することが可能となる。

本願第 5 の発明によれば、第 1 の発明において、A V データを構成するデータブロックにタイムスタンプを付加し、1 つ以上のタイムスタンプ付データブロックをまとめて R T P パケットのペイロード部または H T T P パケットのペイロード部にマッピングする。たとえば、A V データが M P E G - T S の場合、各 T S パケットにタイムスタンプを付加し、複数のタイムスタンプ付 T S パケットをまとめて R T P または H T T P 上にマッピングする。たとえば、各 T S パケットに付加するタイムスタンプのクロックは M P E G のシステムクロック周波数を用いることができる。T S パケットに付加されたタイムスタンプより、M P E G - T S のネットワーク伝送により P C R に付加した伝送ジッターを除去して、受信側での M P E G システムクロックの再生を行うことが可能となる。

本願第 6 の発明によれば、第 1 の発明において、A V データのパケット化は、受信側からの制御により、R T P または H T T P プロトコルで行うことを切替え制御すること。たとえば、A V データのパケット化は、受信側の A V データ出力がディスプレイ充てに出力される場合は遅延の小さい R T P プロトコルを用い、受信側の A V データ出力が記録メディアに蓄積される場合は再送によりパケット落ちを低減する H T T P プロトコルを用いる。この様に、切替え制御することにより受信側でディスプレイに出力する場合は低遅延での A V コンテンツの伝送が可能となり、また、受信側で蓄積する場合はパケットロスによる信号欠落が補償された高品質な A V コンテンツの伝送が可能となる。

また、本願第 1 から第 6 までの発明によれば、ネットワークを用いた A V コンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（A V データコンテンツ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送される A V データの販売、課金が可能となり、安全性の高い B - B、B - C のコンテンツ販売流通が可能となる。

また、本願第 3 から第 6 までの発明によれば、A V コンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通り C P U を用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データである A V データに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価な C P U や大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

【産業上の利用可能性】

【0 0 1 1】

本願によれば、デジタル放送やDVDディスクのコピー制限コンテンツを、コンテンツの著作権者によって設定されたコピー制御情報を継承しながらIPネットワークを用いて違法コピーを回避しつつ安全に伝送することが可能となる。たとえば、一般家庭において、1階の今にあるデジタルチューナーやDVDレコーダから2回の寝室にあるディスプレイに映画などのプレミアムコンテンツを伝送することが可能となる。

【発明を実施するための最良の形態】

【0 0 1 2】

まず最初に本願発明の位置付けを明確にするために適用されるシステム例の概略について説明する。図1は本願発明を適用するシステムの一例である。

図1において、パケット送信機器(101)およびパケット受信機器(103)は、本願第1, 2, 3, 4および5の発明実施部である(以下、本願発明部)。101は送信機器、102はルータ、103は受信機器である。送信機器(101)には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム(MPEG-TSなどコンテンツ)が入力され、以下の手順1から3に基づき、通信が実行される。

手順1) 送受信パラメータの設定を行なう。

【0 0 1 3】

(1-1) 送受信機器のMACアドレス、IPアドレス、TCP/UDPポート番号等を設定。

【0 0 1 4】

(1-2) 送信信号の種別、帯域を設定。QoSエージェントとして動作する送信機器(101)と受信機器(103)、QoSマネージャとして動作するルータ(102)との間でIEEE 802.1Q(VLAN)規格を用いたネットワークの運用に関する設定を実施。

【0 0 1 5】

(1-3) 優先度の設定(IEEE 802.1Q/pによる運用)

手順2) 認証と鍵交換：

(2-1) 認証と鍵交換を行なう。たとえば、DTCP方式を用いることもできる。

手順3) ストリーム伝送：

(3-1) 送信機器と受信機器間での暗号化されたストリームコンテンツ(MPEG-TS)の伝送
なお、コンテンツの入力信号としてMPEG1/2/4などにおけるMPEG-TS, MPEG-PS, MPEG-ES, MPEG-PESなどがある。ここでは、例ではMPEG-TSを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム(ISO/IEC 13818)、DV(IEC 61834、IEC 61883)、SMPTE 314M(DV-based)、SMPTE 259M(SDI)、SMPTE 305M(SDTI)、SMPTE 292M(HD-SDI)等で規格化されているストリーム、さらには、一般的なAVコンテンツも適用可能である。さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。

次に、上記手順2の認証と鍵交換に関して補足説明する。図2において、送信機器と受信機器間はIPネットワークにより接続されている。まず、送信機器から受信機器へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。受信機器は、コンテンツのコピー保護情報の解析を行い、使用する認証方式を決定して認証要求を送信機器に送る。これらの処理を通して送信機器と受信機器は認証鍵を共有する。次に、送信機器は認証鍵を用いて交換鍵を暗号化して受信機器に送り、受信機器で交換鍵が復号される。送信機器では暗号鍵を時間的に変化させるために、時間的に変化させる鍵変更情報を

生成し、受信機器に送信する。送信機器では、交換鍵と鍵変更情報より暗号化鍵を生成して、MPEG-TSをこの暗号化鍵を用いて暗号化手段で暗号化して受信機器に送信する。受信機器は受信した鍵変更情報を交換鍵より復号鍵を復元する。受信機器ではこの復号鍵を用いて暗号化されたMPEG-TS信号を復号する。

図3は本方式をイーサネット(R)を用い2階建ての家庭に適用した場合の一例である。図3において、301は1階のネットワーク構成、302は2階のネットワーク構成である。303は1階に設置されインターネットと接続されるルータ、304は2階に設置されているスイッチングハブである。304はルータ(303)とスイッチングハブ(304)を接続するイーサネット(R)ネットワークである。家庭内の全てのイーサネット(R)ネットワークの帯域は100Mbpsである。1階のネットワーク構成の詳細としては、ルータ(303)にはテレビ(TV)、パソコン(PC)、DVDレコーダが100Mbpsのイーサネット(R)で接続され、また、エアコン、冷蔵庫がECHONETで接続されている。また、2階では、スイッチングハブ(304)にテレビ(TV)、パソコン(PC)、DVDレコーダが100Mbpsのイーサネット(R)で接続され、また、エアコンがECHONETで接続されている。なお、ECHONETは「エコーネットコンソーシアム」(HYPERLINK "http://www.echonet.gr.jp/" http://www.echonet.gr.jp/)で開発されている伝送方式である。

図3において、パソコン(PC)、DVDレコーダ、ルータ(301)およびスイッチングハブ(304)は、IEEE 802.1Q(VLAN)に対応している。すなわち、ルータ(301)およびスイッチングハブ(304)において、各ポートのデータレートが全て同じ(例えば100Mbps)場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ(あるいは、スイッチングハブ)内部で失われず全て出力ポートに出力される。スイッチングハブでは、たとえば8個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

図3において、家庭内の全てのイーサネット(R)の帯域が100Mbpsであるため、1階と2階間のネットワーク305の帯域も100Mbpsである。1階と2階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク305上を流れるデータのデータレート合計が100Mbpsを超える可能性があり、MPEG-TSの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。たとえば、MPEG-TSストリームの伝送優先度をファイル転送データの伝送優先度よりも高くすると、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することが可能となる。

前述したルータ、またはスイッチングハブにおける伝送速度制限機構は、データ流入制御により実現できる。すなわち、ルータ(あるいは、スイッチングハブ)の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジューリング方式WFQ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する情報は、戸田巖著、「ネットワークQoS技術」、平成13年5月25日(第1版)、オーム社刊の第12章などに記述されている。

【実施例1】

【0016】

本願第1の発明について説明する。図4は本願第1の発明の packets 送受信手段に関するブロック図である。401はAKE手段を用いた暗号化による packets 送受信手段である。ここで、AKEは、「認証と鍵交換」(Authentication and Key Exchange)の略語であり、AKE手段は認証手段413と暗号化鍵の交換手段414を具備する。AKE手段(402)に対してAKE設定情報を入力され、このAKE設定情報に関連した情報、たとえばコピー保護情報と暗号化鍵変更情報、が packets 化手段(403)に入力され、TCP/IPプロトコルのヘッダーを付加され、さらに、フレーム化手段409においてMAC(Media Access Control)ヘッダーが付加されイーサネット(R)フレームに変換し、送信フレームとしてネットワークに出力される。ここで、packets 化手段(403)は送信条件設定手段(404)により決定された送信パラメータにより、入力データの packets 化および送信を行なう。なお、送信条件設定手段(404)には、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段(ローカル)と受信手段(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力され、packets 化手段(403)およびフレーム化手段(409)で生成するヘッダーやペイロードデータなどを設定する。

受信側では、ネットワークより入力する信号がフレーム受信手段(410)でMACヘッダーを元にフィルタリングされ、IP packets として packets 受信手段(405)に入力される。packets 受信手段(405)ではIP packets ヘッダーなどの識別によりフィルタリングを行い、AKE手段(402)に入力される。これにより送信側のAKE手段と、受信側のAKE手段がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、AKE手段の設定手順に従い、認証と鍵交換を実行することができる。

【0017】

送信側と、受信側で認証と鍵交換が成立すれば、暗号化したAVデータを送信する。送信側では、MP EG-TS信号を暗号化データ生成手段(406)に入力して、暗号化データ生成手段(406)内の暗号化手段411でMP EG-TS信号を暗号化した後、前述したEMI、シード情報(シード情報のすべてのビット、または、O/Eなど一部のビット)などのAKE情報を暗号化情報ヘッダー付加手段412で付加する。さらに、この信号を packets 化手段(403)に入力し、送信条件などのパラメータを用いてTCP/IPプロトコルのヘッダーを付加する。さらに、フレーム化手段409において、802.1Q(VLAN)方式を用いて、MACヘッダーを付加しイーサネット(R)フレームに変換して、送信フレームとしてネットワークに出力する。ここで、MACヘッダー内のTCI(Tag Control Information)内のPriority(ユーザ優先度)を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

受信側では、ネットワークより入力する信号がフレーム受信手段(410)でMACヘッダーを元にフィルタリングされ、IP packets として packets 受信手段(405)に入力される。packets 受信手段(405)で packets ヘッダーなどの識別によりフィルタリングされ、暗号化データ復号手段(407)に入力され、暗号化情報ヘッダーの除去と暗号の復号化が行われ、復号されたMP EG-TS信号が出力される。

【0018】

なお、送信条件設定手段(404)には、受信状況を送信側にフィードバックするためのデータが入力され、IP packets の packets 化手段(403)およびイーサネット(R)フレームのフレーム化手段(409)で生成するヘッダーおよびペイロードデータを設定する。

【0019】

次に、図5のプロトコルスタックを用い上記手順を補足説明する。図5の送信側におい

て、まず送信側から受信側へ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求を送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報（機器ID、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新情報を生成し、受信側に送信する。コンテンツであるMPEG-TSは暗号化鍵により暗号化される。そして暗号化されたMPEG-TSは、AVデータとしてTCP（またはUDP）パケットのペイロードとしてTCPパケットが生成される。さらにこのTCPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット（R）MACフレームが生成される。なお、MACとしてはイーサネット（R）であるIEEE 802.3だけでなく、無線LAN規格のIEEE 802.11のMACにも適用できる。

【0020】

さて、イーサネット（R）MACフレームは、イーサネット（R）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（R）MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP（またはUDP）パケットが抜き出される。そして、TCP（またはUDP）パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG-TS（コンテンツ）が復号され出力される。

【0021】

以上、MPEG-TS信号などのAVストリームを送信機器で暗号化して、IPパケットをネットワークにより伝送し、受信機器で元の信号に復号することが可能である。なお、図3において、スイッチングハブを用いたネットワークポロジを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。たとえば、1階と2階の間のネットワーク305の帯域を、従来の実施例で説明した100Mbpsから1Gbpsに拡張することによって、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することができる。たとえば、市販されている100Mbpsのポートを8つ、1Gbpsのポートを1つ持ったスイッチングハブを用い、1階と2階を結ぶネットワーク305に1Gbpsのポートを接続し、残りの8chの100MbpsのポートにTVなどのAV機器を接続する。100Mbpsのポートは8つなので、8つのポートのデータがそれぞれ最大100Mbpsで入力されて1Gbpsのポートに出力されたとしても、 $100\text{Mbps} \times 8\text{ch} = 800\text{Mbps}$ と1Gbpsより小さいため、8つのポートから入力されたデータはスイッチングハブ内部で失われず全て1Gbpsのポートに出力される。よって、1階で発生したデータは全て2階に伝送することが可能である。また、逆に2階で発生したデータも全て1階に伝送することが可能である。以上の様に、スイッチングハブを用いる場合、ネットワークポロジを工夫することによりストリーム伝送とファイル転送を共存させることができる。

【実施例2】

【0022】

本願第2の発明について説明する。図6は本願第2の発明のブロック図である。図6においては、認証モード決定手段601以外は、図4と同様の構成である。よって以下では新

規な部分について説明する。

図6において、AKE手段(402)に対してAKE設定情報として、認証用のTCPプロトコルのポート番号を図6の管理情報データとして送信条件の設定管理手段404に入力される。ここで、認証用のTCPポート情報は、コンテンツ毎または放送チャンネル毎にアクセス位置を指定するURI、または、Queryにより拡張されたURI情報とにより与える。ここで、URIに主データ部にコンテンツのURI情報、Query部にそのコンテンツの認証情報をマッピングする。これにより、もし、Query部がなければそのコンテンツの伝送には認証が不必要であり、Query部が存在すればそのコンテンツの伝送には認証が必要である様にモード設定することができる。URIとQueryの例は、例えば下記の形式で与えることができる。

【0023】

```
<service>://<host>:<port>/<path>/  
<filename>.<ext>?AKEPORT=<port2>
```

ここで、<host>:<port>/<path>/<filename>.<ext>はAVコンテンツのURIとファイル名称を表しており、?以下のQuery部における<port2>は認証用ポート番号を表している。ただし、認証用ポートのIPアドレスはAVコンテンツのIPアドレスと同じ場合である。

【0024】

送信側はこのURIとQueryで認証の実行モード情報を受信側に与える。受信側はWEBブラウザやUPnP-AVのCDS(コンテンツディレクトリサービス)を用いて、上記のURIとQuery情報を受け取り、認証モードを決定することができる。その他の動作は、第1の実施例と同様である。

【実施例3】

【0025】

本願第3の発明について説明する。図7は本願第3の発明のブロック図である。図7においては、

送信条件の設定管理手段404に入力されるAVデータの入力ソース情報(放送、蓄積)以外は、図6と同様の構成である。よって以下では新規な部分について説明する。

図7において、送信条件の設定管理手段404に入力されるAVデータの入力ソース情報(放送、蓄積)では、送信条件の設定管理手段404において必要データを抽出され、暗号化データ生成手段406内の暗号化情報ヘッダー付加手段に入力され、以下の様に暗号化情報ヘッダー付加制御が行われる。

図7において、送信条件の設定管理手段404に入力されるAVデータの入力ソース情報(放送、蓄積)としては、たとえば次のケースが考えられる。

(ケース 1) 前記AVデータがコピーフリーコンテンツを放送する放送チャンネルを受信したコンテンツの場合。この様な放送チャンネルの例としては、たとえば、アナログ放送であるVHF、UHF、またはBSアナログ放送の放送チャンネルがある。

(ケース 2) 前記AVデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャンネルを受信したコンテンツの場合。この様な放送チャンネルの例としては、たとえば、BSデジタル放送の有料チャンネルやCATV放送による有料チャンネルがある。この一定期間でもコピーフリーでないコンテンツを放送する放送チャンネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびEPNフラグ付きコピーフリーが放送内容により時々刻々と切り替わるのが特徴である。

ここで、一定期間でもコピーフリーでないコンテンツを放送する放送チャンネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信装置または受信ユーザであることを認証された場合に行われるように制御できる。この認証の例としては、日本のデジタル衛星放送のB-CASカード、または米国のCATV放送で使用するPODカードなどのセキュリティモジュールによる認証が考えられる。

また、暗号化情報ヘッダーの付加制御は、たとえば以下の様に行なう。すなわち、コピー

フリーコンテンツを放送する放送チャネルを受信した場合には付加しない。また、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信した場合には付加する。さらに、A V データが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない。そして、A V データが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する。

以上の様に暗号化情報ヘッダーの付加制御を行うことにより、著作権者が設定したA V コンテンツのC C I (コピー制御情報) をネットワーク伝送においても継承して伝えていくことができる。さらに、送信側と受信側で暗号化情報ヘッダーの付加制御のルールを揃えることにより異機種間での動作互換性を確保することができる。

【実施例 4】

【0 0 2 6】

本願第 4 の発明について説明する。図 8 は本願第 4 の発明のブロック図である。図 8 においては、送信キュー制御手段 (8 0 1)、第 1 キュー手段 (8 0 2)、および第 2 キュー手段 (8 0 3) 以外は、図 4 と同様の構成である、よって以下では新規な部分について説明する。

図 8 において、A K E 手段 (4 0 2) に対して A K E 設定情報を入力され、この A K E 設定情報に関連した情報 (たとえば、コピー保護情報と暗号化鍵変更情報)、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報 (ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段 (ローカル) と受信手段 (リモート) における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段 (4 0 3) に入力され、T C P / I P プロトコル処理をして、第 1 キュー手段 (8 0 2) に入力される。また、送信側では M P E G - T S 信号を暗号化手段 (4 0 6) に入力して、M P E G - T S 信号を暗号化した後、この暗号化された M P E G - T S 信号をパケット化手段 (4 0 3) に入力し、T C P / I P プロトコル処理をして、第 2 キュー手段 (8 0 3) に入力される。

送信キュー制御手段 (8 0 1) は、第 1 キューと第 2 キューにデータが存在する場合、どちらのデータを優先して出力するかを制御を行なう。通常状態では、一般データよりも M P E G - T S などのコンテンツデータを優先制御して出力する。たとえば、送受信機器間で M P E G - T S を低レイテンシ (低遅延) で伝送する場合には、M P E G - T S 用バッファも小さくなるため、オーバーフローが発生しやすい。送信側で M P E G - T S バッファがオーバーフローしそうな場合、あるいは、受信側からフィードバックされた情報を参照して受信側の M P E G - T S のバッファがアンダーフローしそうなことが判明した場合には、M P E G - T S データを優先出力する様に第 2 キュー手段の優先度を更に適応的に上げることにより、これらバッファ破綻を回避できる。

ただし、受信側機器 (リモート機器) の再生、停止などの機器制御応答をより速くするには、第 1 キューの優先度を適応的に上げればよいが、これでは前述した M P E G - T S バッファのオーバーフローまたはアンダーフローが発生する可能性がある。

バッファのオーバーフローやアンダーフローを避け、かつ、受信側機器 (リモート機器) の再生、停止などの機器制御応答をより速くする別手段として、機器制御用パケットだけはキューを経由せずに直接フレーム化手段に出力する方法により、迅速な制御応答が実現できる。あるいは、機器制御用パケットに対して第 3 キューを新たに用意する方法により、迅速な制御応答が実現できる。

【0 0 2 7】

受信側の動作は第 1 の実施例と同様である。

【実施例 5】

【0 0 2 8】

本願第 5 の発明の実施形態について説明する。図 9 はその実施例のブロック図である。図 9 においては、パケット化手段 (4 0 3) 内の第 1 のパケット化手段 (9 0 1) および

第2の packets 化手段(902)、packets 受信手段(405)内の第1の packets 受信手段(903)および第2の packets 受信手段(904)以外は図8と同様の構成である、よって以下では新規な部分について説明する。

図9において、AKE手段(402)に対してAKE設定情報を入力し、このAKE設定情報に関連した情報(たとえば、コピー保護情報と暗号化鍵変更情報)、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段(ローカル)と受信手段(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが第1の packets 化手段(701)に入力されプロセッサを用いたソフトウェア処理でTCP/IPプロトコル処理をされ、第1キュー手段(803)に入力される。

送信側ではMP EG-TS信号を暗号化手段(406)に入力して、MP EG-TS信号を暗号化した後、この暗号化されたMP EG-TS信号を packets 化手段(403)に入力し、ハードウェア処理によりUDP/IPプロトコルの処理をされ、第2キュー手段(804)に入力される。

送信キュー制御手段(802)は、第1キューと第2キューの双方にデータが存在する場合、前述の実施の形態2と同様に、2つのキューからのデータ出力に関して優先制御を行なう。

さて、受信側では、ネットワークより入力する信号がフレーム受信手段(410)でMACヘッダーを元にIP packets がフィルタリングされる。ここでは、上記第1の packets 化手段(901)から出力されたIP packets が第1の packets 受信手段(903)に入力され、上記第2の packets 化手段(902)から出力されたIP packets がおよび第2の packets 受信手段(904)に入力される。第1の packets 受信手段(903)ではプロセッサを用いたソフトウェア処理でTCP/IPプロトコルの受信処理を行い、AKE手段(402)または受信条件の設定管理手段(408)に出力する。また、第2の packets 受信手段(904)ではハードウェア処理によりUDP/IPプロトコルの受信処理を行い、復号手段(407)に入力され、暗号が復号されたMP EG-TSが出力される。

次に、図10のプロトコルスタックを用い、上記手順を補足説明する。図10においては、MP EG-TSなどAVデータのトランスミッション層がUDPである以外は、図5と同様の構成である、よって以下では新規な部分について説明する。図8の送信側において、コンテンツであるMP EG-TSは暗号化鍵K_cにより暗号化される。そして暗号化されたMP EG-TSは、前述したEMI、シード情報とともにAVデータとして、ハードウェアによりUDP packets のペイロードとしてUDP packets が生成される。さらにこのUDP packets はIP packets のデータペイロードとして使用され、IP packets が生成される。

なお、送信側から受信側への、EMI、シード情報の伝送方法としては、たとえば、専用の別 packets を生成して伝送することも可能であり、暗号鍵復元がさらに困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなど公衆網において、リアルタイムに伝送されるAVデータの暗号化パラメータが変化させたり、別 packets で送ると、コンテンツの盗聴、漏洩をより困難にすることができる。管理制御データに関しては図5の例と同様に、ソフトウェア処理によりTCP packets が生成され、IP packets 化される。

【0029】

さて、イーサネット(R)MACフレームは、イーサネット(R)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット(R)MACフレームからIP packets がフィルタリングされる。さらにIP packets からUDP packets が抜き出され、UDP packets からAVデータが抜き出され、交換鍵とシード情報より復元された復号鍵K_cにより、MP EG-TS(コンテンツ)が復号され出力される。

【0030】

図11は、MPEG-TSをIPパケット化、さらにイーサネット(R)フレーム化して伝送する場合のパケット形式の一例である。188バイトのMPEG-TSに6バイトのタイムコード(TC)を付加して194バイトの単位を作る。TCは42ビットのタイムスタンプと6ビットのベースクロックID(BCID)により構成される。BCIDによりタイムスタンプの周波数情報を表すことができる。たとえば、(ケース1)BCIDが0x00の場合は、タイムスタンプの周波数情報はない、(ケース2)BCIDが0x01の場合は、タイムスタンプの周波数情報としては27MHz(MPEG2のシステムクロック周波数)である、(ケース3)また、BCIDが0x02の場合は、タイムスタンプの周波数情報としては90kHz(MPEG1で使用されるクロック周波数)である、(ケース4)BCIDが0x03の場合は、タイムスタンプの周波数情報としては24.576MHz(IEEE 1394で使用されるクロック周波数)である。(ケース5)BCIDが0x04の場合は、タイムスタンプの周波数情報としては100MHz(イーサネット(R)で使用される周波数)である、という様にBCIDでタイムスタンプの周波数情報を表すことができる。194バイト単位データを2つあわせて暗号化して、更に14バイトの暗号化情報ヘッダーと合わせてRTPプロトコルのペイロードとする。ここで、暗号化情報ヘッダーは、4ビットのEMIと、64ビットのシード情報と12ビットのReserved Dataにより構成される。RTPパケットはUDPおよびIPプロトコルによりパケット化された後、イーサネット(R)フレーム化される。イーサネット(R)ヘッダとしては、図11に示す様に、標準的なイーサネット(R)ヘッダーとIEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダーの両方をサポートする。なお、IEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダーにおけるTCIフィールドの中の3ビットのPriorityフラグにより、イーサネット(R)フレームの優先度を設定することができる。

【0031】

以上により、送受信機器間でMPEG-TS信号を暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。また、一般データは一時的にバッファ手段に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。また、データ量の小さい第1のパケット化手段はマイコンなど安価なプロセッサで処理できる。さらに、ハードウェア処理により、受信処理においても、イーサネット(R)フレームを受信して、3層のIPヘッダー、4層のUDPヘッダを同時に検査することもできる。MPEG-TSパケットと一般データパケットを分離し、MPEG-TSパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信ができる。

【0032】

パケットの送信タイミング、あるいは2つの送信データキューからのデータ送信割合をソフトウェアではなくハードウェアで制御するとクロック単位で完全な送出制御が可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

ここで、本願第4の発明に戻り、その第2の実施形態について説明する。図12はその実施例のブロック図であり、AKE手段にDTCF方式を用いる場合の一例である。また、図13はパケット化手段(403)内の第1のパケット化手段(1301)および第2のパケット化手段(1302)、パケット受信手段(405)内の第1のパケット受信手段(1303)および第2のパケット受信手段(1304)におけるパケット処理について

の説明図である。

さて、図 1 2 において、A K E 手段 (4 0 2) 内の D T C P 情報生成手段 (1 2 0 1)、A K E コマンド受信処理手段 (1 2 0 1)、A K E コマンド送信処理手段 (1 2 0 3)、交換鍵生成手段 (1 2 0 4)、暗号鍵生成手段 (1 2 0 5)、暗号鍵変更情報生成手段 (1 2 0 6)、復号鍵生成手段 (1 2 0 7) 以外は図 9 と同様の構成である、よって以下では新規な部分について説明する。図 1 2 においては、以下のステップで D T C P 方式により暗号化コンテンツの伝送が行なわれる。

(ステップ 1) コピー制御情報が D T C P 情報生成手段 (1 2 0 1) に入力される。

(ステップ 2) まず、ソース側でコンテンツの送信要求を発生させ、D T C P 情報生成手段 (1 2 0 1) よりコンテンツの保護モード情報 (E M I 情報) が第 1 のパケット化手段 (9 0 1) に出力され、パケット化された後、ソースに送信される。

(ステップ 3) そして、受信側 (シンク) は、第 1 のパケット受信手段 (9 0 3) より A K E コマンド受信処理手段 (1 2 0 2) に入力されたコンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、A K E 送信処理手段 (1 2 0 3) を通じて認証要求をソースに送る。

(ステップ 4) ソースとシンク間で D T C P 所定の処理が行なわれ、認証鍵が共有される。

(ステップ 5) 次に、ソースは A K E 送信処理手段において、認証鍵を用いて交換鍵を暗号化して第 1 のパケット化手段を経由してシンクに送り、シンクにおいて A K E コマンド受信処理手段から与えられる情報により、交換鍵生成手段 (1 0 0 4) において交換鍵が復号される。

(ステップ 6) ソースでは暗号鍵を時間的に変化させるために、暗号化鍵生成手段において、時間的に変化するシード情報 (O / E) を生成し、D T C P 情報生成手段 (1 2 0 1)、および第 1 のパケット化手段 (7 0 1) を経由してシンクに送信する。

(ステップ 7) ソースでは、暗号化鍵生成手段 (1 2 0 5) において交換鍵とシード情報より暗号化鍵を生成して、暗号化手段で M P E G - T S を暗号化して第 2 のパケット化手段 (9 0 2) に出力する。

(ステップ 8) シンク内部の、暗号鍵変更情報生成手段 (1 2 0 6) は第 1 のパケット受信手段 (9 0 3) よりシード情報を受信し、復号鍵生成手段 (1 2 0 7) はこのシード情報と交換鍵生成手段 (1 2 0 4) の情報より復号鍵を復元する。

(ステップ 9) シンクでは、この復号鍵を用いて復号手段 4 0 7 において、暗号化された M P E G - T S 信号を復号する。

【0 0 3 3】

図 1 1 は、パケット化手段 (4 0 3) 内の第 1 のパケット化手段 (7 0 1) および第 2 のパケット化手段 (7 0 2)、パケット受信手段 (4 0 5) 内の第 1 のパケット受信手段 (7 0 3) および第 2 のパケット受信手段 (7 0 4) におけるパケット処理について説明する図である。

第 1 のパケット化手段 (7 0 1)、入力データを内部で R T C P または R T S P プロトコル、T C P または U D P プロトコル、さらに I P プロトコルによる処理がなされ出力される。なお、R T C P プロトコル (r f c 1 8 8 9) は、ネットワークの実効帯域幅や遅延時間などを受信装置より送信装置に送り、送信装置は報告された通信状態に合わせて R T P で送信するデータの品質を調整して送信することもできる。また、R T S P プロトコル (r f c 2 3 2 6) は、再生、停止、早送り、などの制御コマンドを送ることもでき、A V ファイルよりデータをダウンロードしながらコンテンツを再生することが可能である。

【0 0 3 4】

第 2 のパケット化手段 (7 0 2) は、内部で入力データを R T P プロトコル、U D P プロトコル、そして I P プロトコルでそれぞれ処理して I P パケットを出力する。

【0 0 3 5】

また、第 1 のパケット受信手段 (7 0 3) は、内部でフィルタリングなど I P 受信処理、T C P または U D P プロトコルの受信処理、さらに、R T C P または R T S P プロトコ

ルによる受信処理がなされたデータが出力される。

【0036】

また、第2の packets 受信手段（704）は、内部でフィルタリングなど IP 受信処理、UDP プロトコルの受信処理、さらに、RTP プロトコルの受信処理がなされたデータが出力される。

【0037】

以上により、送受信機器間で MPEG-TS 信号を DTCP 方式により暗号化してリアルタイム伝送が可能となるだけでなく、第2の packets 化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信 packets の送り残しや受信 packets の取りこぼしが発生しない。また、データ量の小さい第1の packets 化手段はマイコンなど安価なプロセッサで処理できる。

さらに、本願第4の発明の第3の実施例について説明する。図12はその発明のブロック図である。本実施例では図14の第2の packets 化手段（1402）、および第2の packets 受信手段（1404）以外は図13と同様の構成である、よって以下では新規な部分について説明する。

【0038】

第2の packets 化手段（1402）は、内部で入力データにエラー訂正処理を行ない、RTP プロトコル、UDP プロトコル、そして IP プロトコルでそれぞれ処理して IP packets を出力する。

【0039】

また、第2の packets 受信手段（1404）は、内部でフィルタリングなど IP 受信処理、UDP プロトコルの受信処理、RTP プロトコルの受信処理、さらにエラー訂正復号処理を行いエラー訂正されたデータが出力される。

【0040】

図15は本願第4の発明の第3の実施例におけるプロトコルスタックの説明図であり、送信処理では、AV データにエラー訂正符号が付加され（ECC エンコード）、UDP プロトコルに渡される。また、受信処理では、UDP プロトコル処理よりデータを受け取り、エラー訂正後に上位層に AV データとして渡される。

【0041】

ここで、エラー訂正処理の例を図16および図17を使用して説明する。図16はエラー訂正方式がリードソロモン方式の場合である。MPEG-TS を2つ単位でエラー訂正インターリーブマトリックスに入力する。なお、各行にはシーケンス番号を2バイト使用する。そして、図16および図17に示す様に、たとえば前述した10バイトの DTCP 情報（EMI 情報4ビット、シード情報64ビット、その他12ビット）を用い、さらに、RTP ヘッダ、UDP ヘッダ、IP ヘッダ、イーサネット（R）ヘッダを付加してイーサネット（R）フレームを構成する。

【0042】

以上により、送受信機器間で MPEG-TS 信号を DTCP 方式により暗号化し、さらにエラー訂正符号を付加しリアルタイム伝送が可能となる。さらに、第2の packets 化手段がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信 packets の送り残しや受信 packets の取りこぼしが発生しない。また、データ量の小さい第1の packets 化手段はマイコンなど安価なプロセッサで処理できる。

【実施例6】

【0043】

本願第6の発明について説明する。図12は本願第5の発明のブロック図である。図12においては、第2の packets 化手段902以外は、第2の packets 受信手段904の内部構成以外は、前述した構成と同様である。よって以下では新規な部分について説明する。図18は本願第5の発明のプロトコルスタックの説明図であり、送信処理では、AV デー

タにエラー訂正符号を付加し（ECCエンコード）、UDPプロトコルに渡す場合と、HTTPプロトコル経由でTCPプロトコルに渡す場合とがある。ここで、AVデータをRTPに渡すかHTTPに渡すかは、受信側からの制御により、RTPまたはHTTPプロトコルで行うことを切替え制御する。たとえば、AVデータの packets 化は、受信側のAVデータ出力がディスプレイ充てに出力される場合は遅延の小さいRTPプロトコルを用い、受信側のAVデータ出力が記録メディアに蓄積される場合は再送により packets 落ちを低減するHTTPプロトコルを用いる。この様に、切替え制御することにより受信側でディスプレイに出力する場合は低遅延でのAVコンテンツの伝送が可能となり、また、受信側で蓄積する場合は packets ロスによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。なお、図18において、受信側のプロトコル処理は、送信側と逆の手順で処理される。

ところで、図19に packets 送信手段、また、図20に packets 送信手段のブロック図を示す。これらは、それぞれ、MPEG-TSなどAVコンテンツの受信機能、または送信機能を省いた構成であり、その他は前述の送受信手段と同じ構成であり、前述した実施の形態に適用できる。送信または受信のみの機器に対して適用可能であり、低コスト化が図れる。

【0044】

なお、上述した実施の形態1から5においては、一般のIPネットワークなど packets の順序性が保証されていない通信網で伝送する場合には、 packets にシーケンス番号を付加して送信し、受信側でシーケンス番号を用いて順序性の保証を行ってもよい。この順序性の保証は、OSIモデルの第4層以上、すなわち、RTPプロトコルやビデオ信号処理などで行なうことができる。

【0045】

なお、送信側側でハードウェア処理され伝送されたAV信号の packets が、ネットワークでフラグメントされないため対策ができる。すなわち、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ（MTU）を検査し、それ以下の packets サイズで伝送すればよい。あるいは、RFCの規格では全ての端末は576バイトのサイズのIP packets を扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のIP packets ではフラグメントが起こらない。したがってIP packets のサイズが576バイト以下となるように、送信側側でハードウェア処理されるAV信号の packets サイズを調整すればよい。なお、送信側側でハードウェア処理されるAV信号の packets にフラグメントが起こらない場合は、受信した packets がフラグメントされていれば全て一般 packets として処理すればよい。なお、イーサネット（R）のIP packets の最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先 packets のフラグメントを起こさせないためにはIP packets の最大値以下でなければならないことは言うまでもない。

【0046】

また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側側でハードウェア処理され伝送されたAV信号の packets のIPヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではIP packets を廃棄させることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数の packets は損失となるが、受信側で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態1から実施の形態6までは、通信網プロトコルとしてイーサネット（R）を例としたがこの限りではない。

【0047】

また、ビデオ信号処理の例として、実施の形態1から5ではMPEG-TSを用いたが、これに限らず本発明で用いる入力データの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム（ISO/IEC 13818）、DV（IEC 61834

、 I E C 6 1 8 8 3) 、 S M P T E 3 1 4 M (D V - b a s e d) 、 S M P T E 2 5 9 M (S D I) 、 S M P T E 3 0 5 M (S D T I) 、 S M P T E 2 9 2 M (H D - S D I) 等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。映像や音声のデータレートは、 C B R (c o n s t a n t b i t r a t e) に限るものではない。さらに、映像や音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本願発明から排除するものではない。

また、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、一定の条件化でリアルタイムより高速の伝送も可能である。

【図面の簡単な説明】

【 0 0 4 8 】

- 【図 1】 本願第 1 の発明を適用するシステムの一例を示す図
- 【図 2】 認証と鍵交換に D T C P 方式を適用する場合のコンテンツ伝送手順の説明図
- 【図 3】 イーサネット (R) を用いる一般家庭に適用した場合の一例の説明図
- 【図 4】 本願第 1 の発明の packets 送信手段のブロック図
- 【図 5】 本願第 1 の発明の protocol stack による説明図
- 【図 6】 本願第 2 の発明の packets 送信手段のブロック図
- 【図 7】 本願第 3 の発明の packets 送信手段のブロック図
- 【図 8】 本願第 4 の発明の packets 送信手段のブロック図
- 【図 9】 本願第 5 の発明の packets 送信手段のブロック図
- 【図 1 0】 本願第 5 の発明の protocol stack による説明図
- 【図 1 1】 本願第 5 の発明における M P E G - T S のイーサネット (R) フレーム構成仕様の例を示す図
- 【図 1 2】 本願第 4 および第 6 の発明における packets 送信手段のブロック図
- 【図 1 3】 本願第 4 の発明の packets 化手段および packets 受信手段の説明図
- 【図 1 4】 本願第 4 の発明の packets 化手段および packets 受信手段の説明図
- 【図 1 5】 本願第 4 の発明の protocol stack による説明図
- 【図 1 6】 エラー訂正方式がリードソロモン方式である場合の説明図
- 【図 1 7】 エラー訂正方式がパリティ方式である場合の説明図
- 【図 1 8】 本願第 6 の発明の packets 化手段および packets 受信手段の説明図
- 【図 1 9】 packets 送信機能の説明図
- 【図 2 0】 packets 受信機能の説明図
- 【図 2 1】 従来例における送信システムの説明図
- 【図 2 2】 従来例における送信ブロックの構成図
- 【図 2 3】 従来例における鍵交換に D T C P 方式を適用する場合のコンテンツ伝送手順の説明図

- 【図 2 4】 従来例における 1 3 9 5 アイソクロナス packets の構成例を示す図

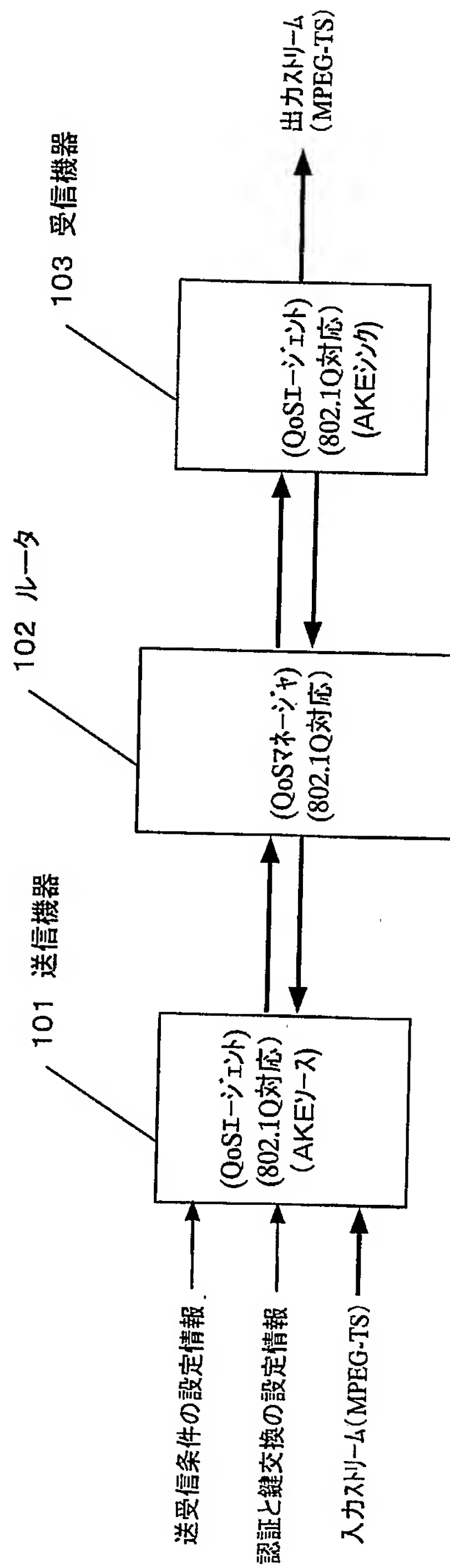
【符号の説明】

【 0 0 4 9 】

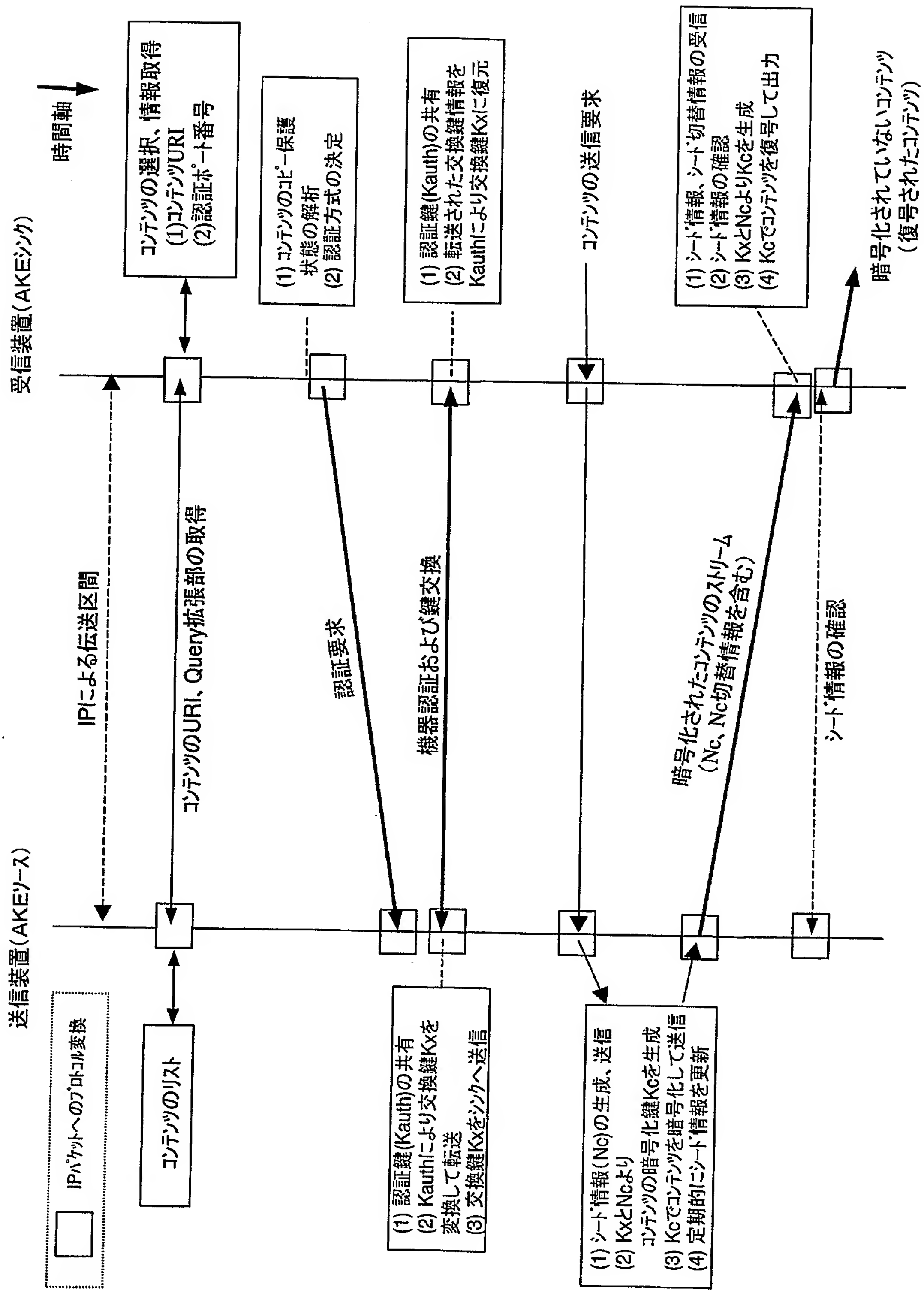
- 1 0 1 packets 送信機器
- 1 0 2 ルータ
- 1 0 3 packets 受信機器
- 4 0 1 packets 送信手段
- 4 0 2 A K E 手段
- 4 0 3 packets 化手段
- 4 0 4 送信条件の設定管理手段
- 4 0 5 packets 受信手段

- 4 0 6 暗号化データ生成手段
- 4 0 7 暗号化データ復号手段
- 4 0 8 受信条件の設定管理手段
- 4 0 9 送信パケットのフレーム化手段
- 4 1 0 フレーム受信手段

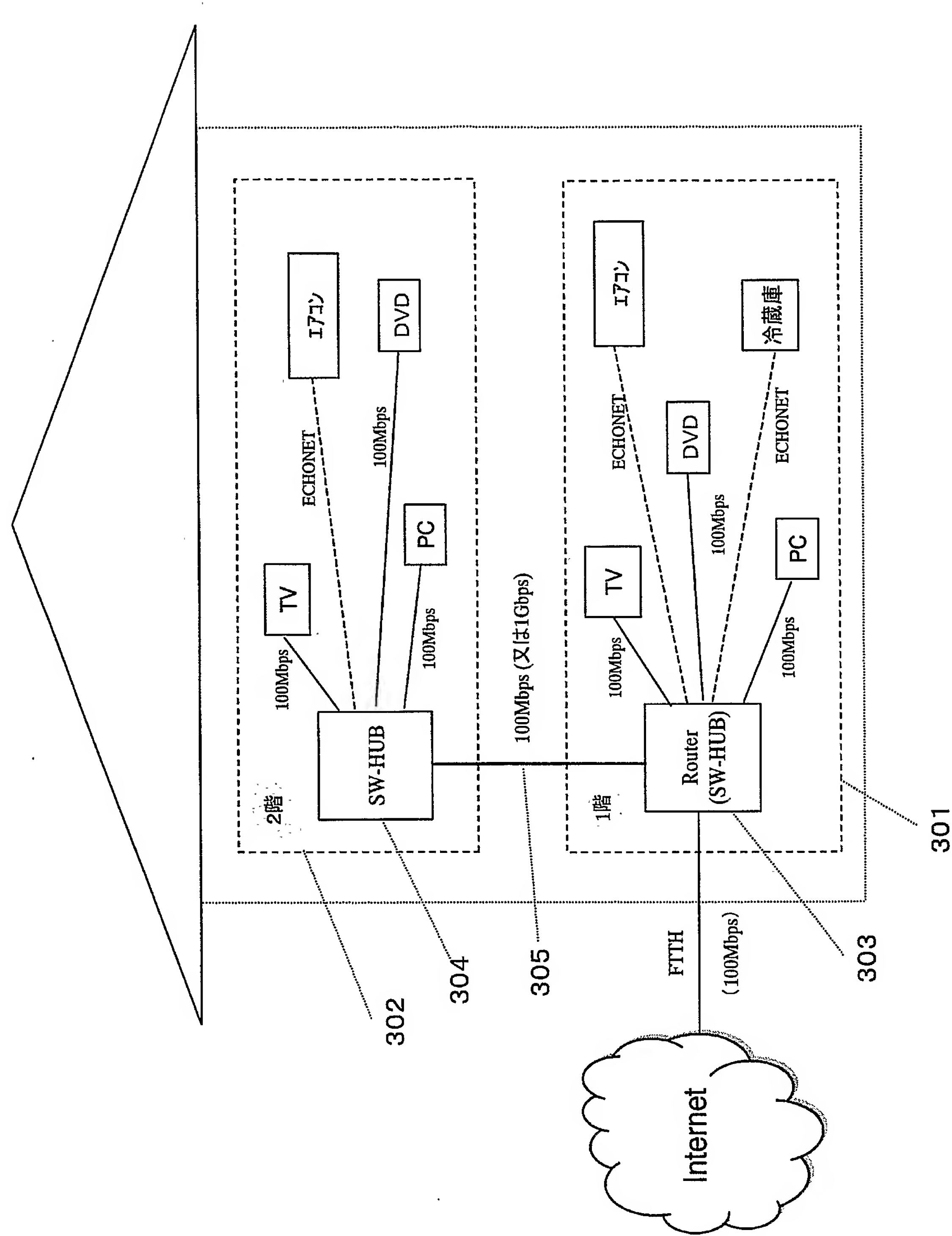
【書類名】 図面
【図 1】



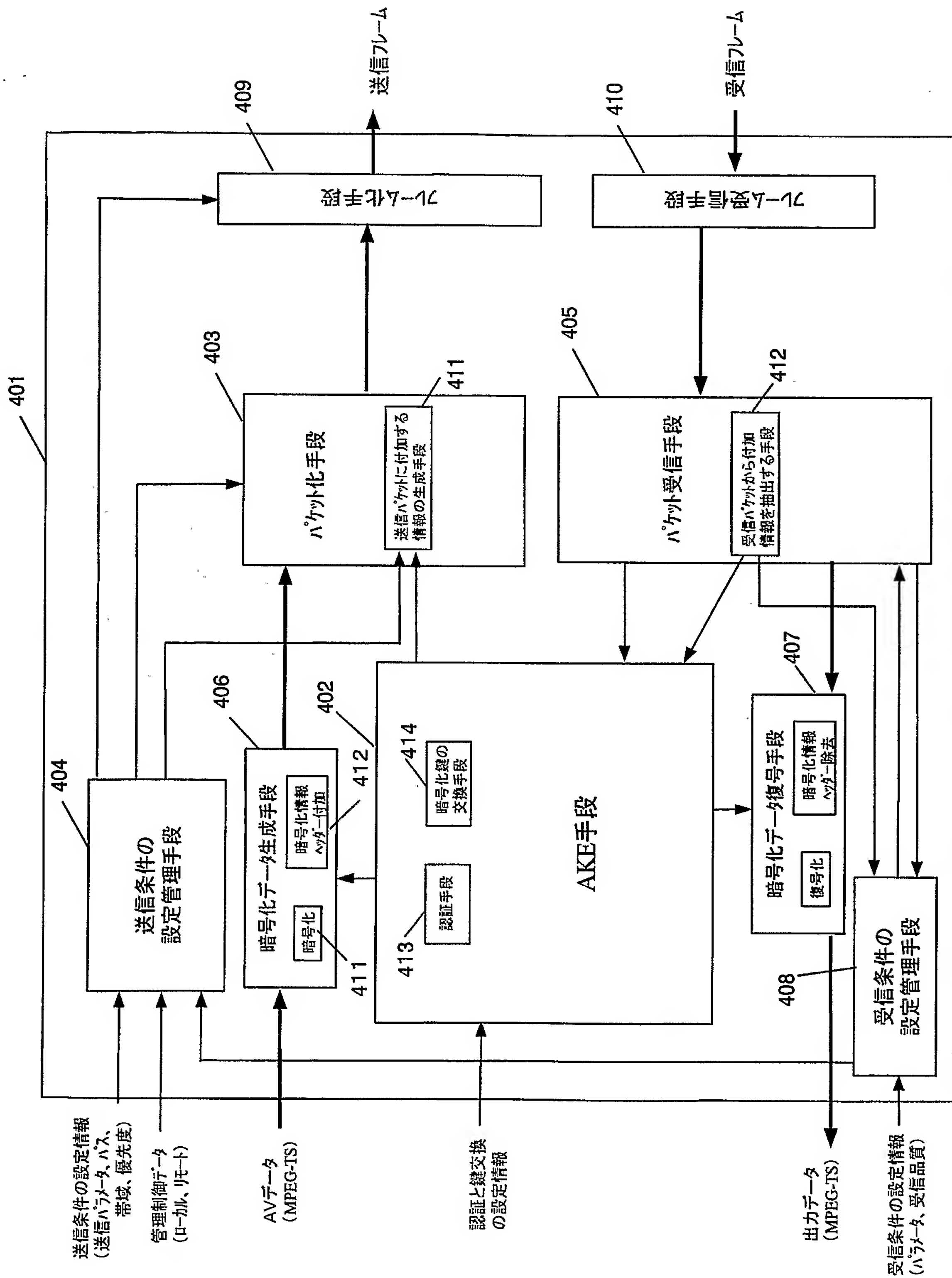
【図 2】



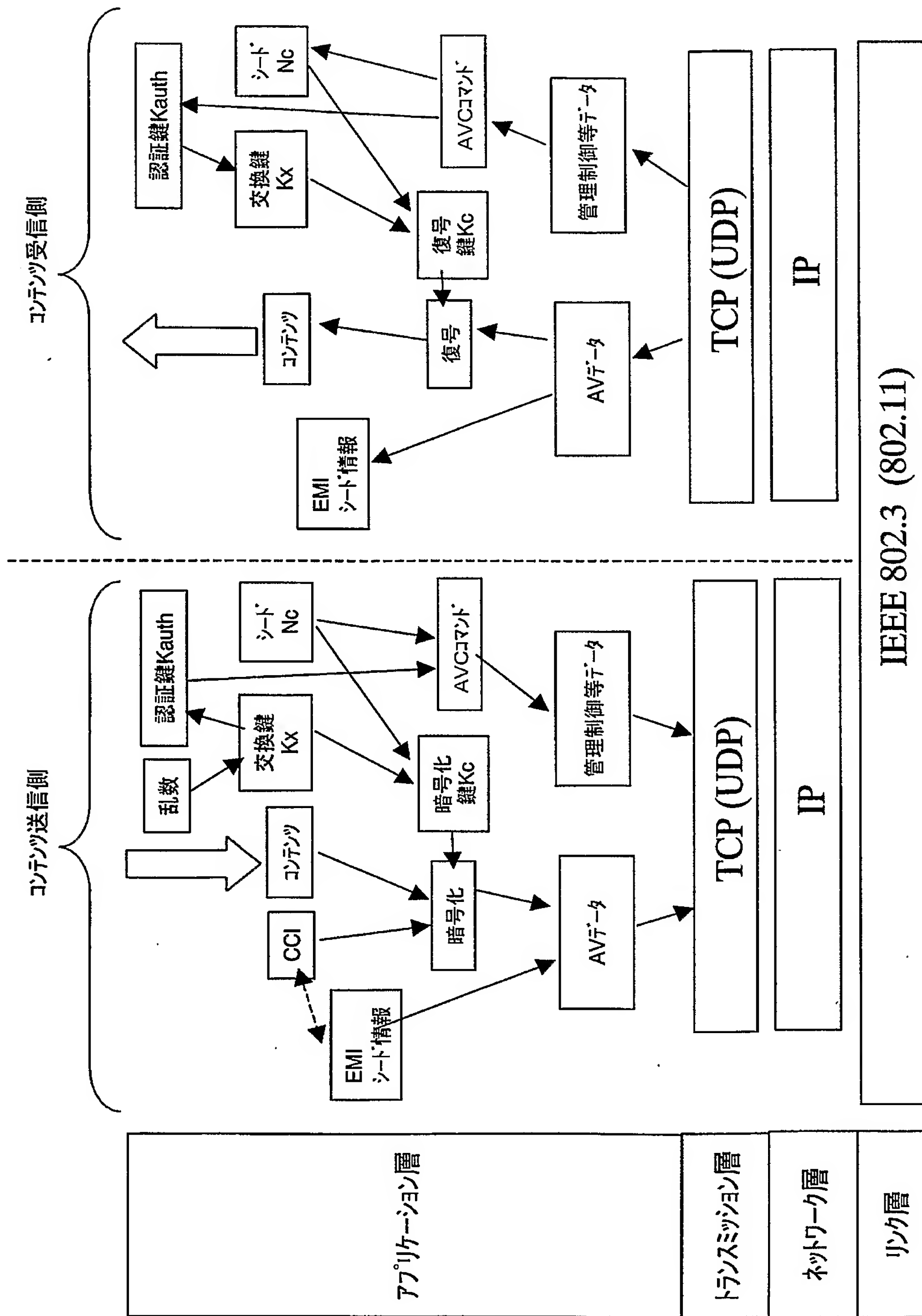
【図 3】



【図 4】

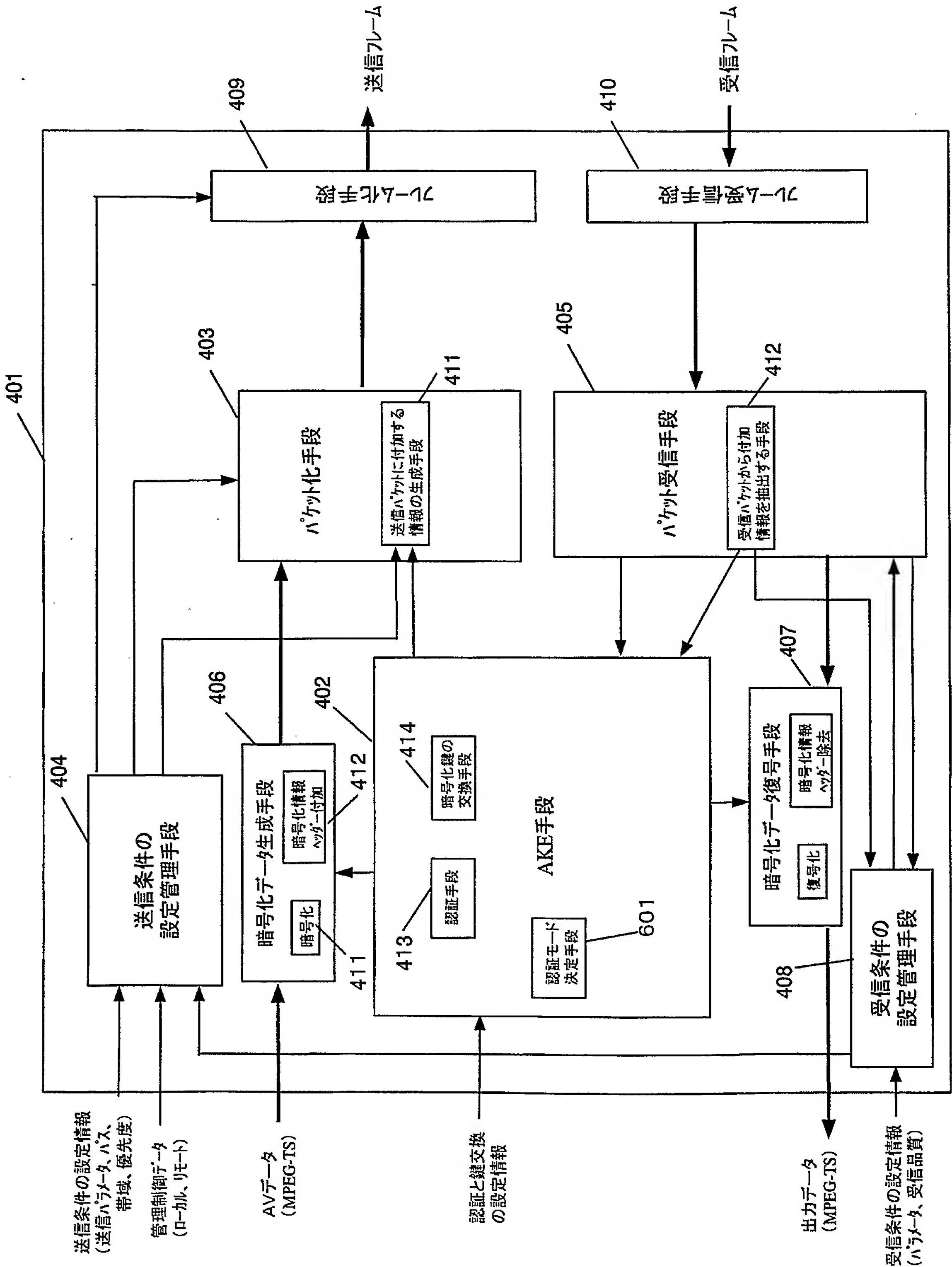


【図 5】

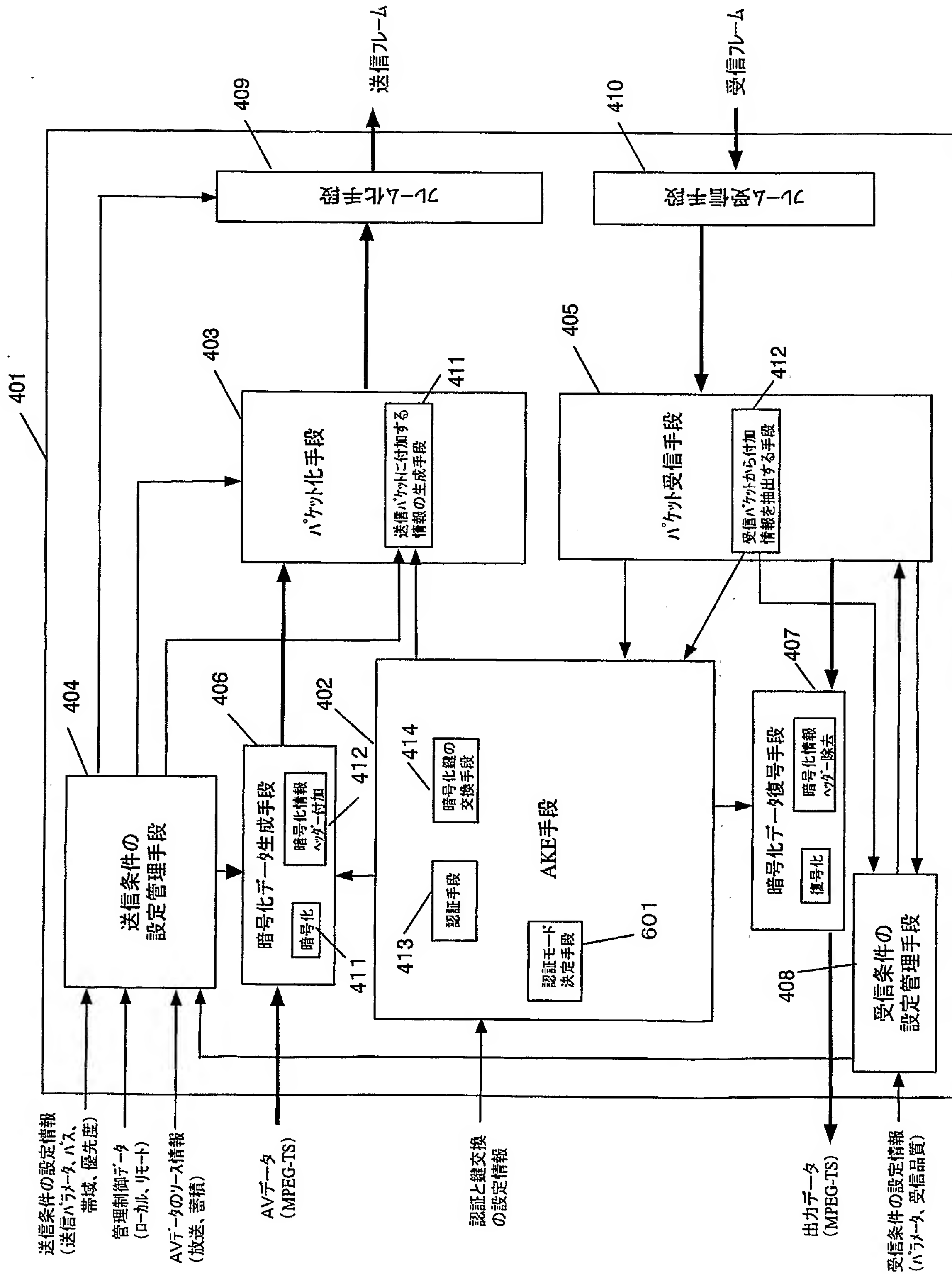


(OSIモデルによる説明)

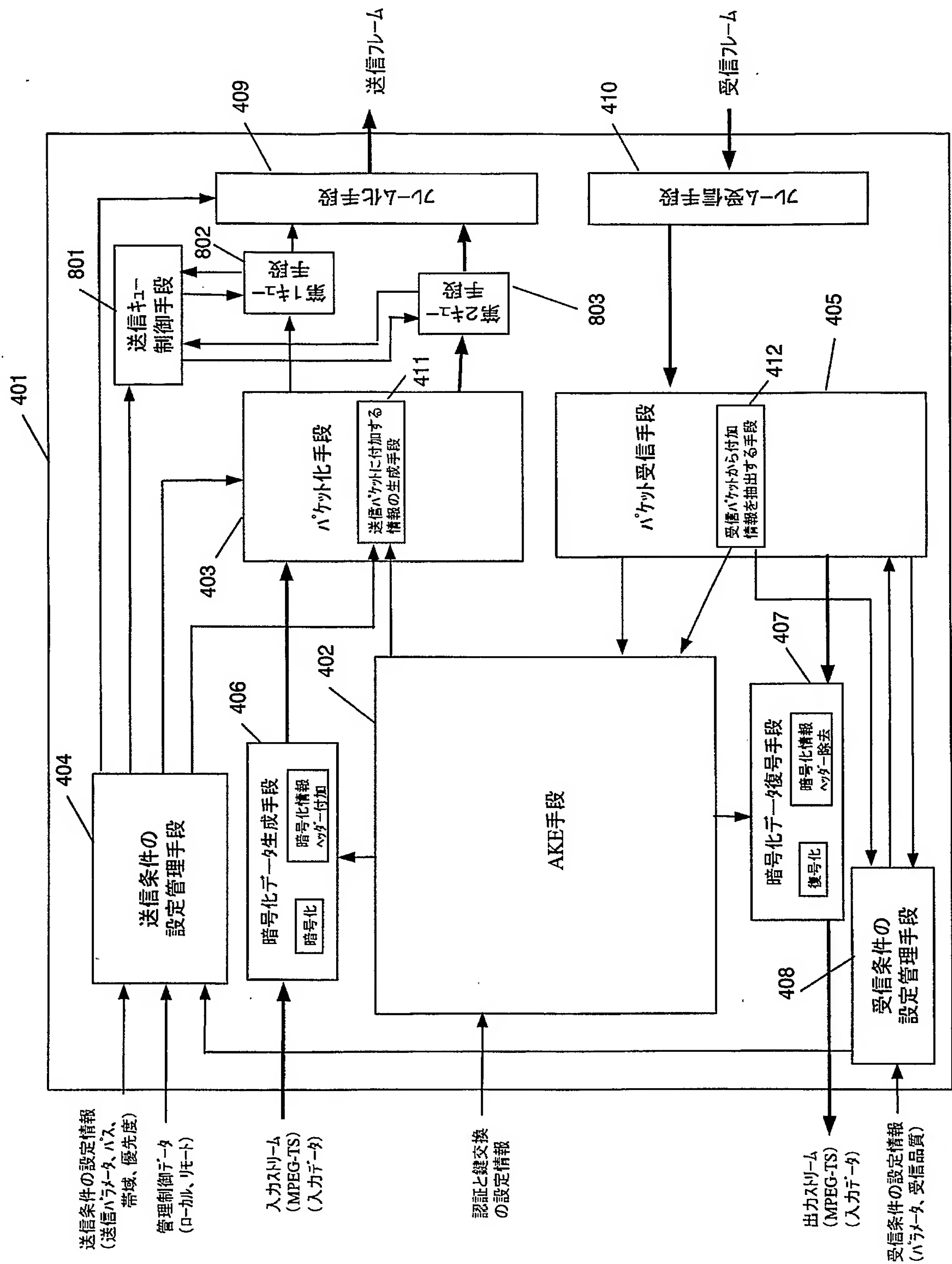
【図 6】



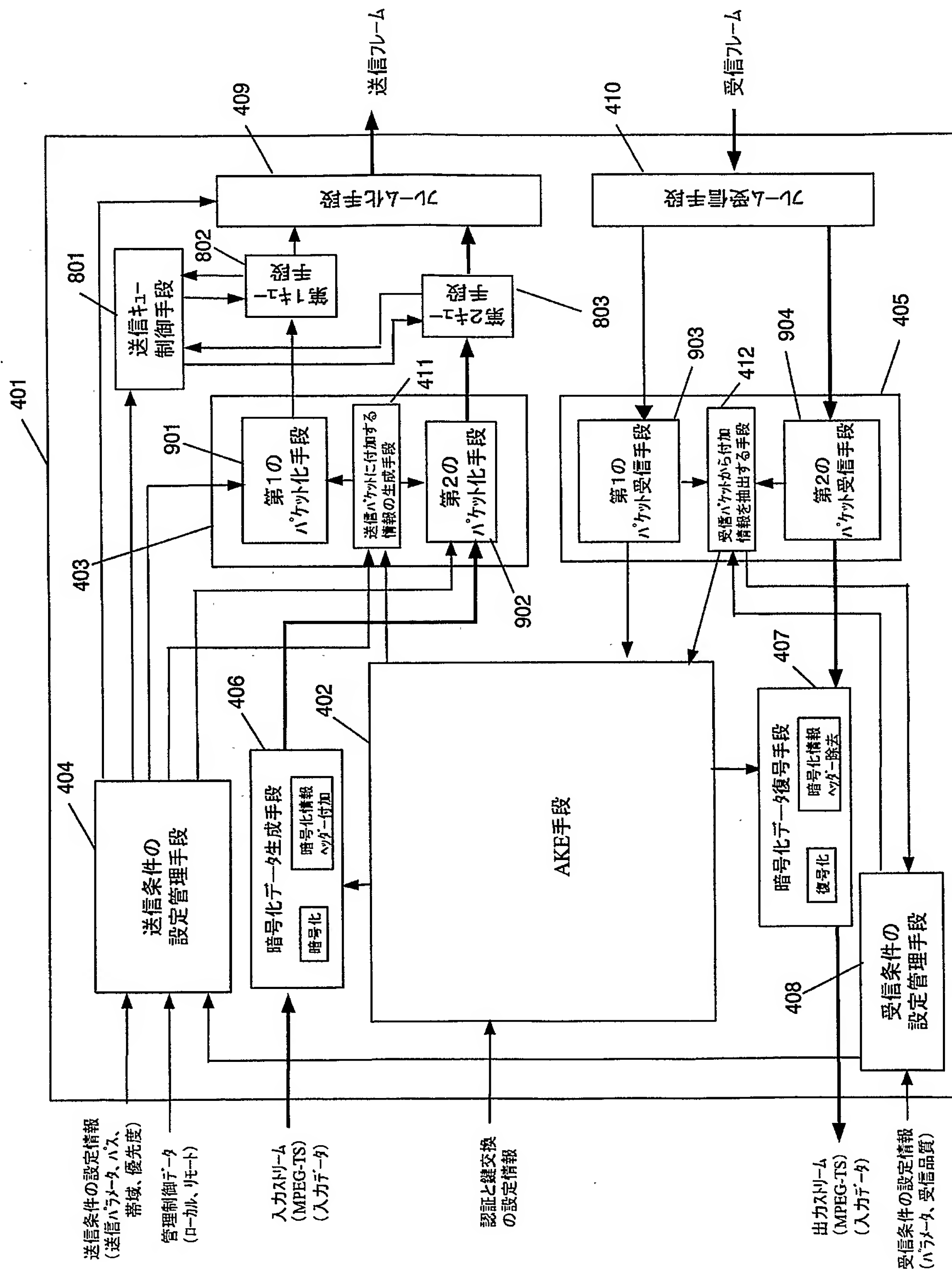
【図 7】



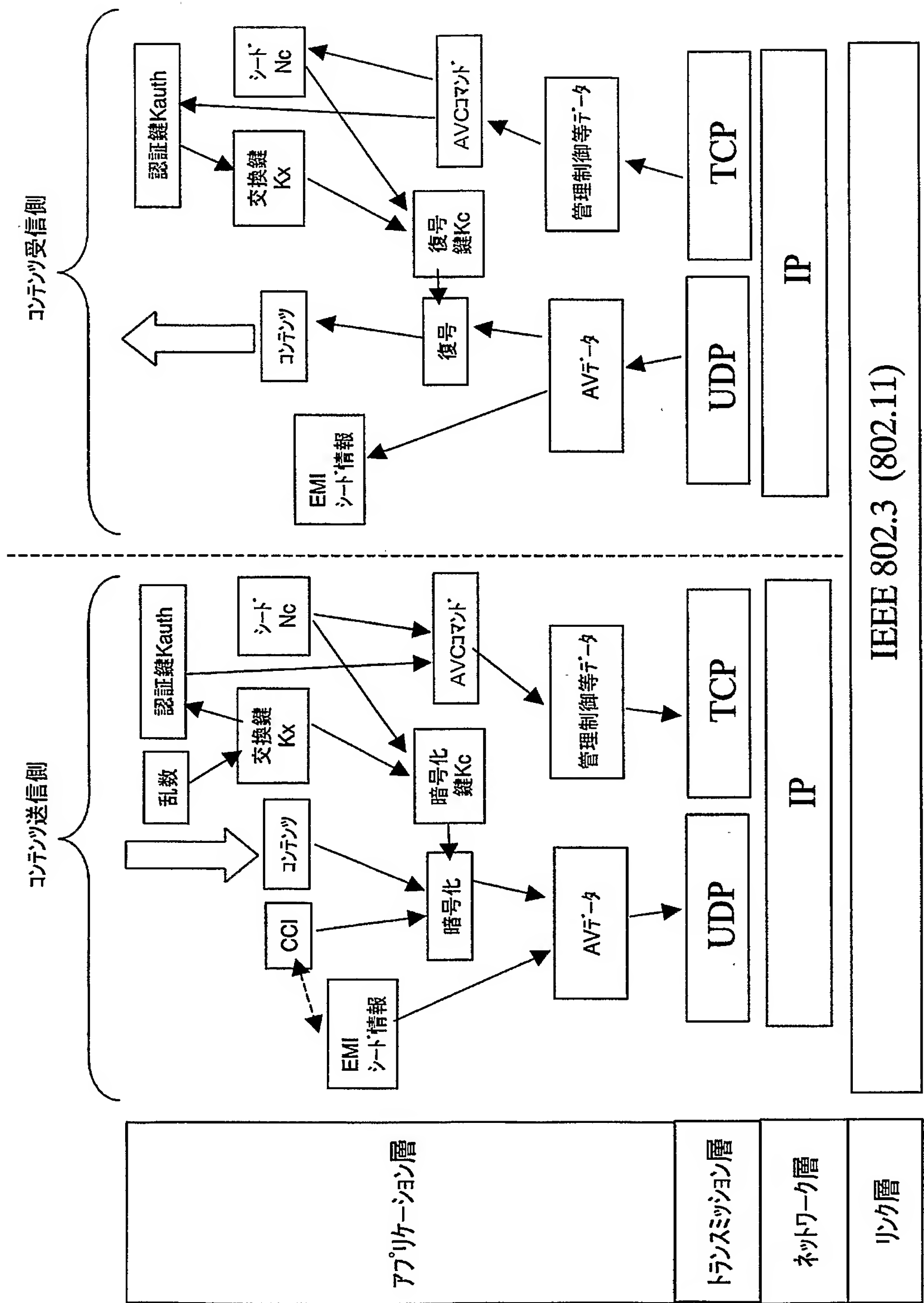
【図 8】



【図 9】

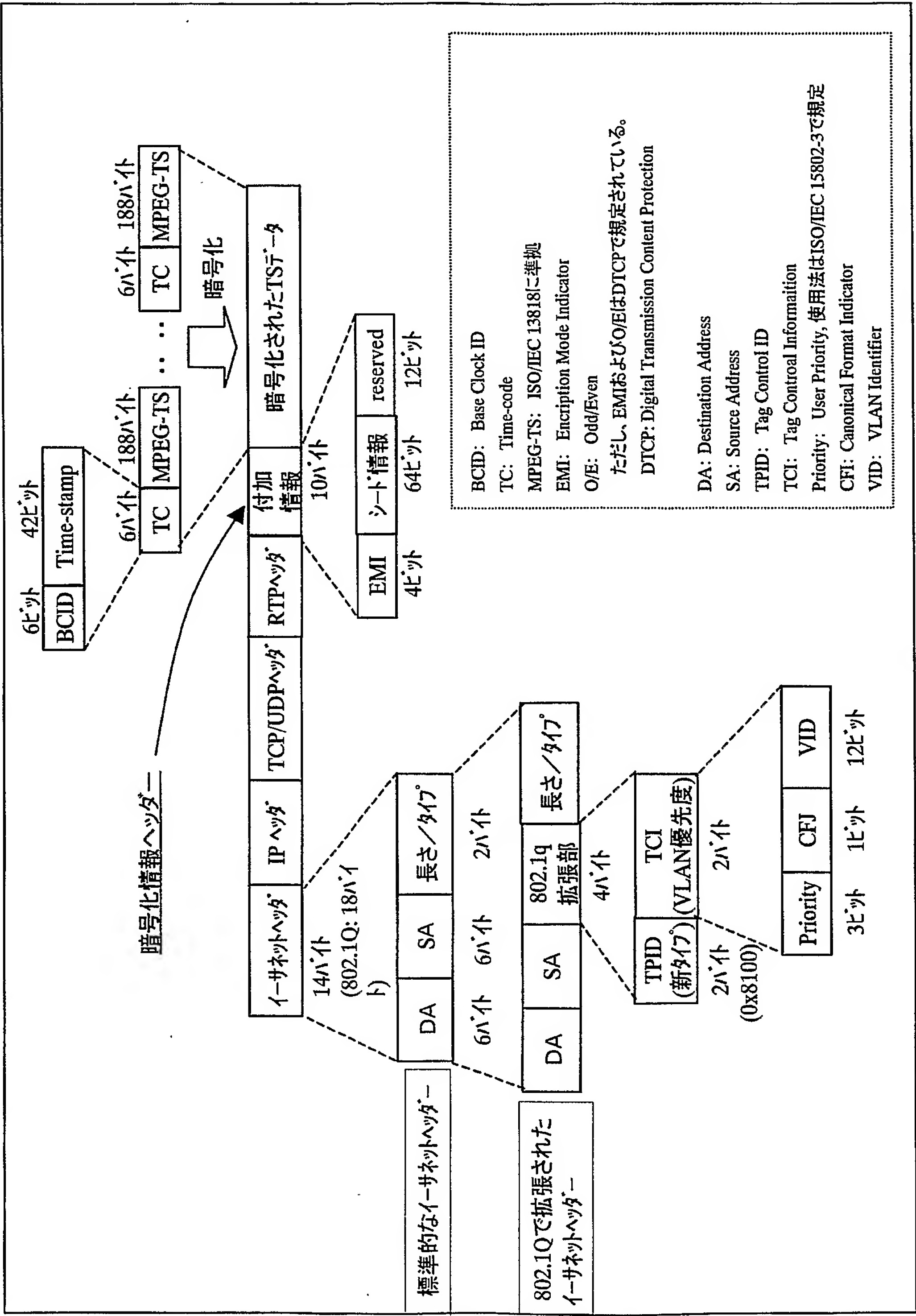


【図 10】

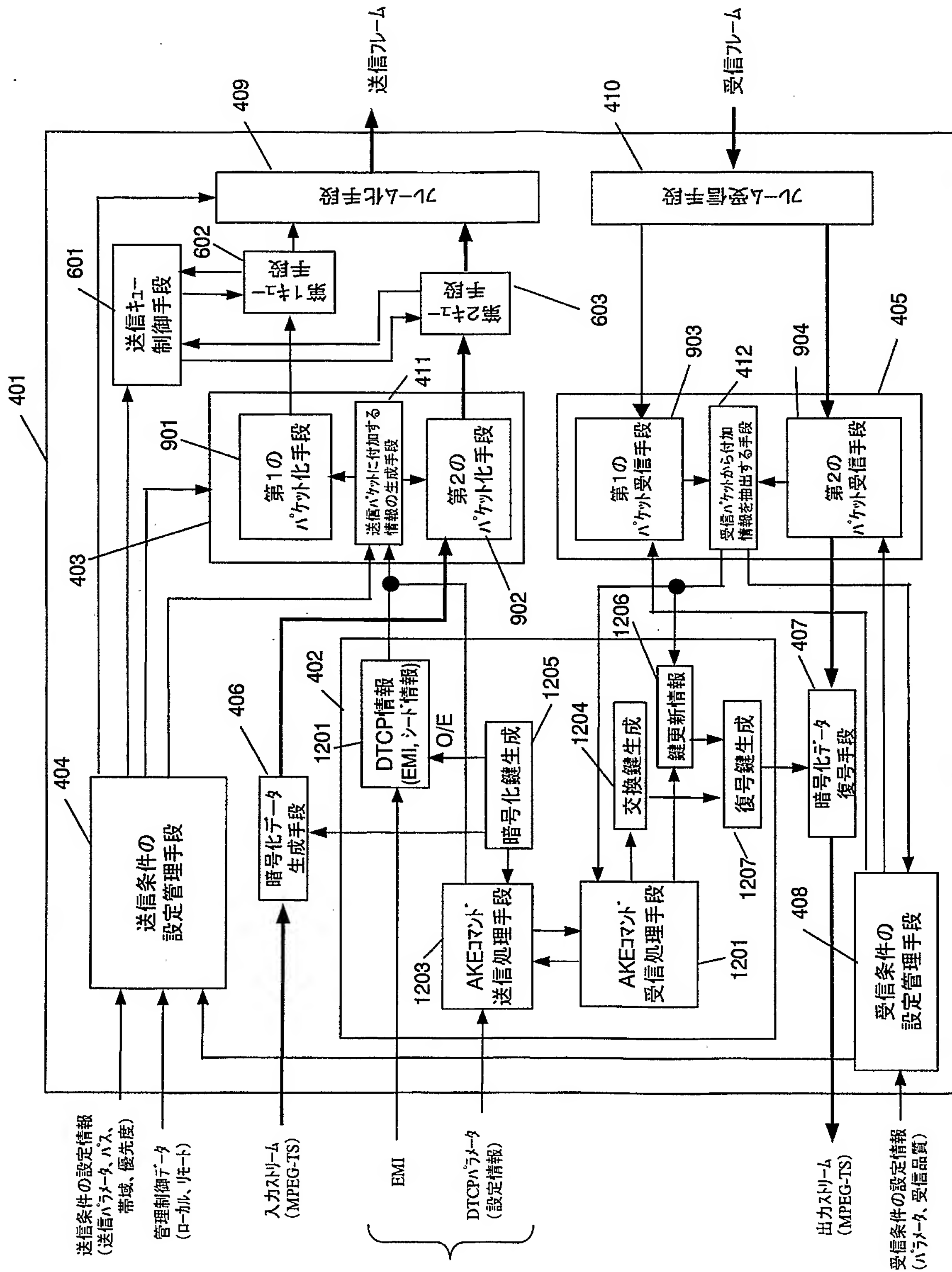


(OSIモデルによる説明)

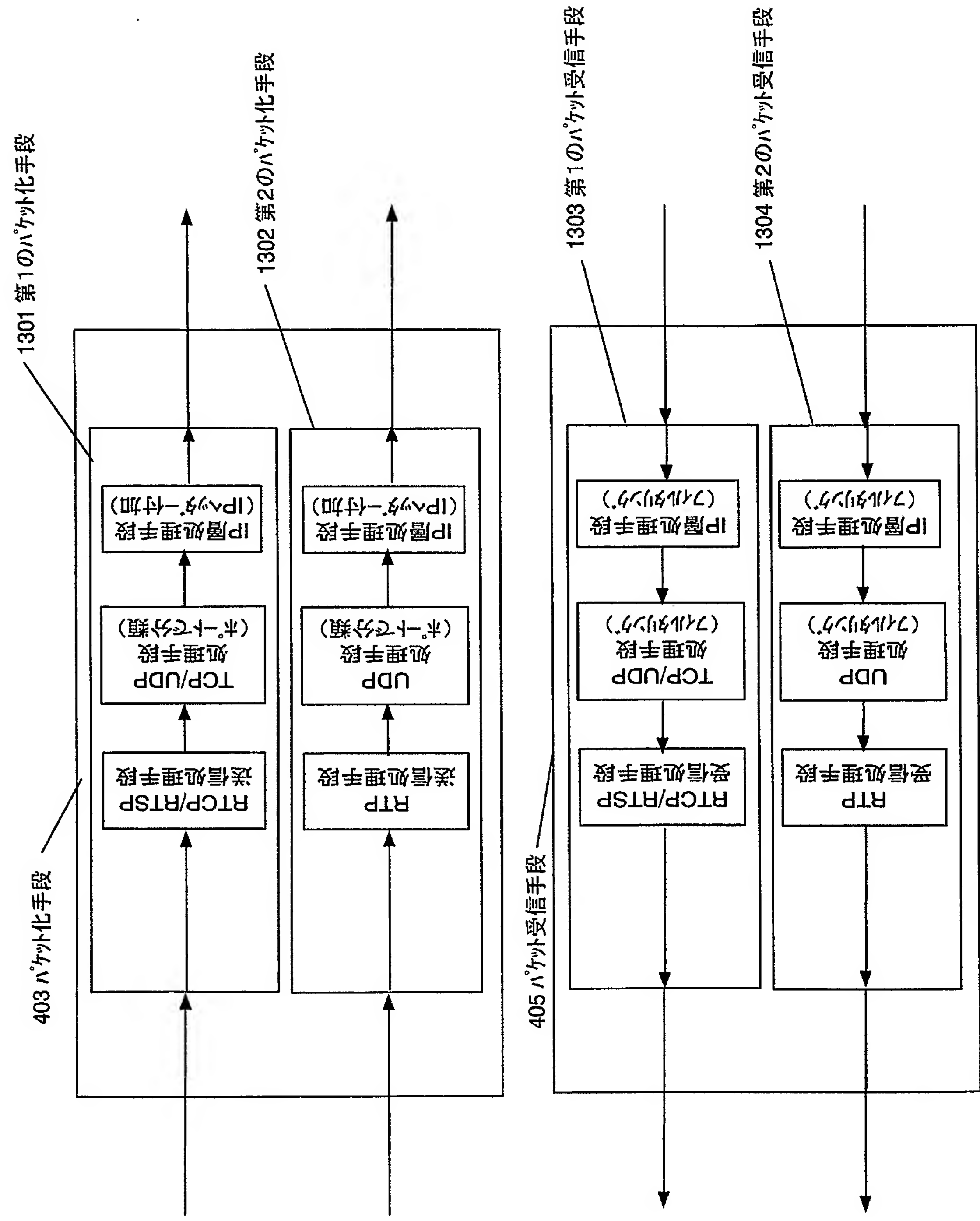
【図 11】



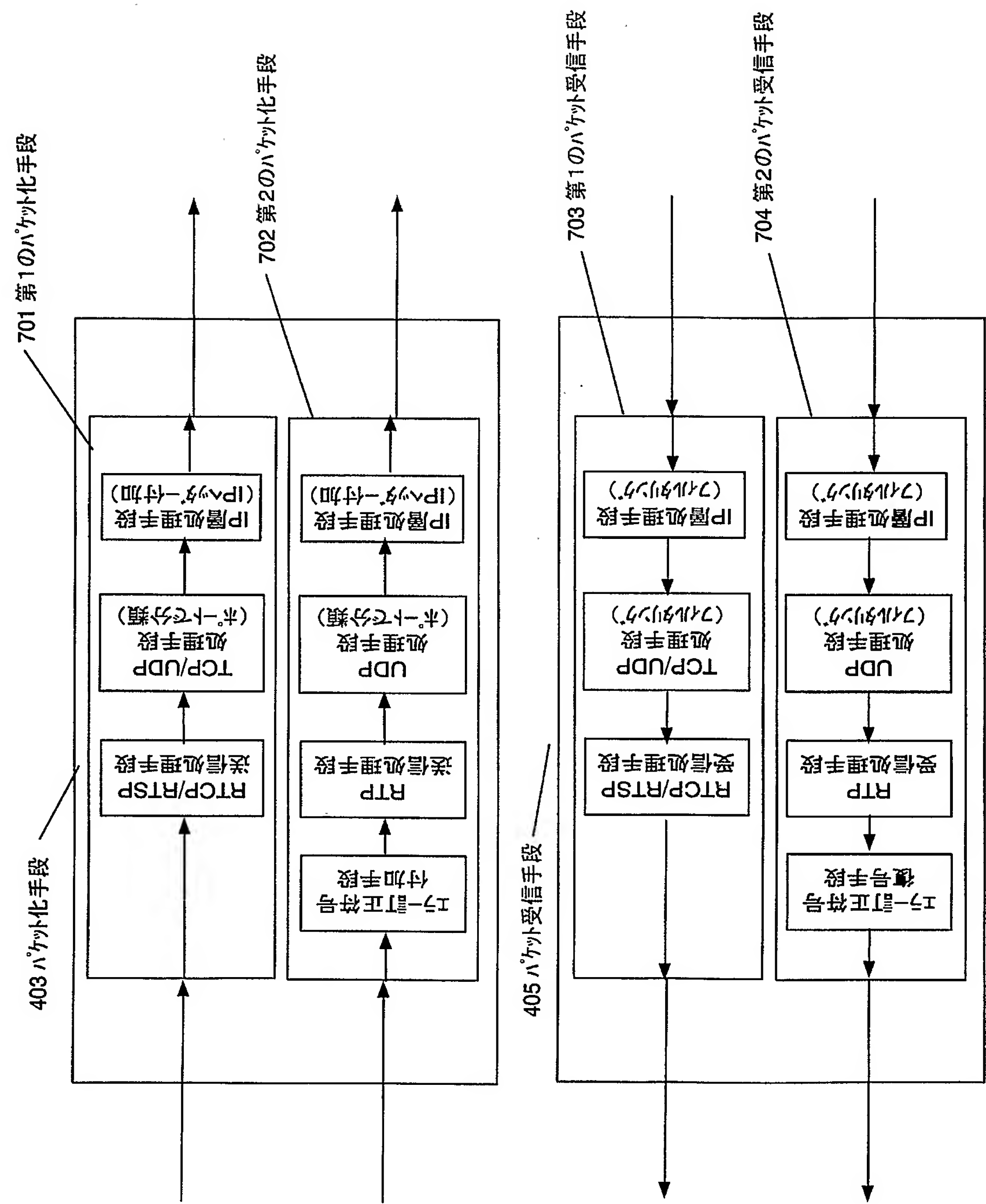
【図 12】



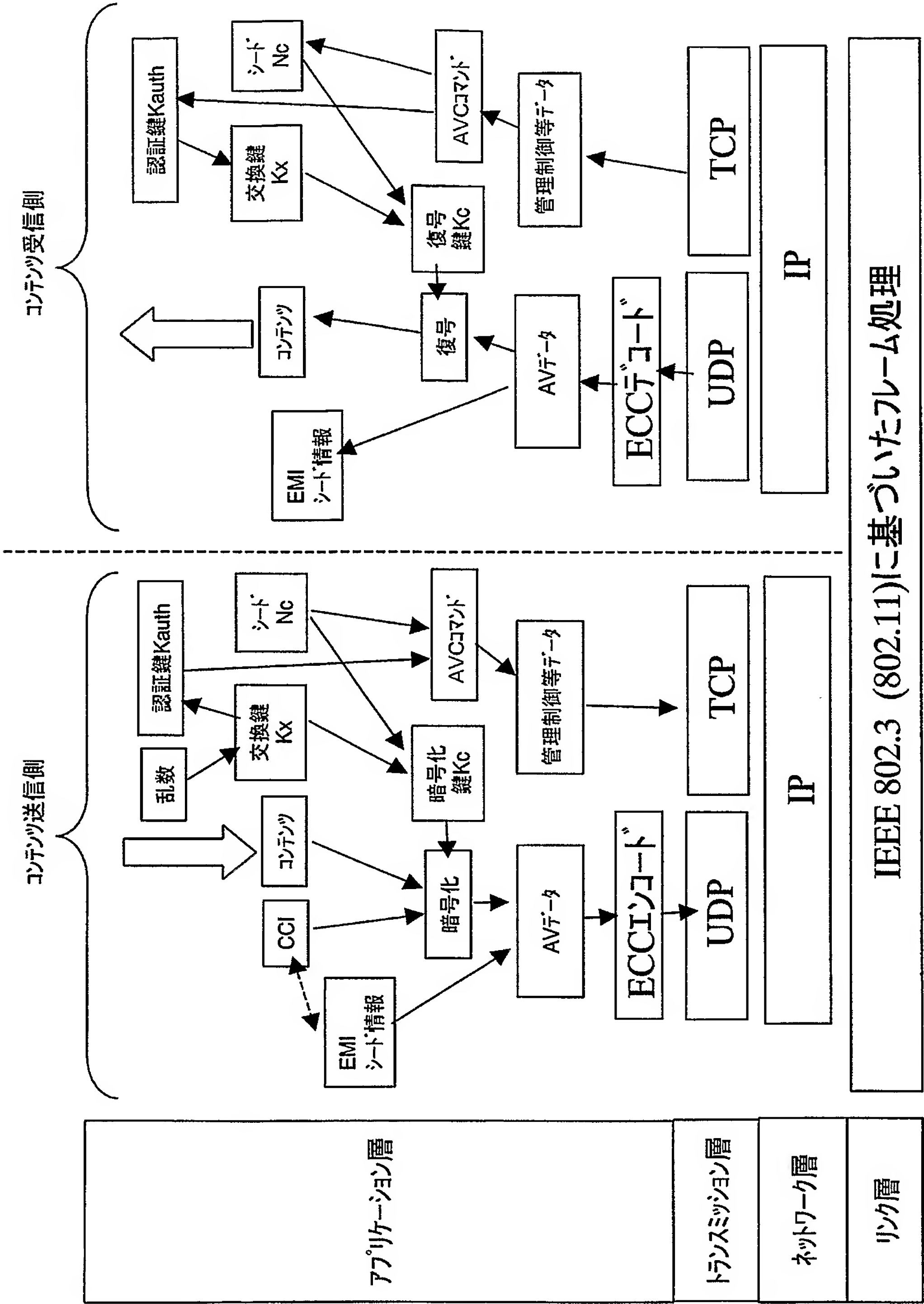
【図 1 3】



【図 1 4】

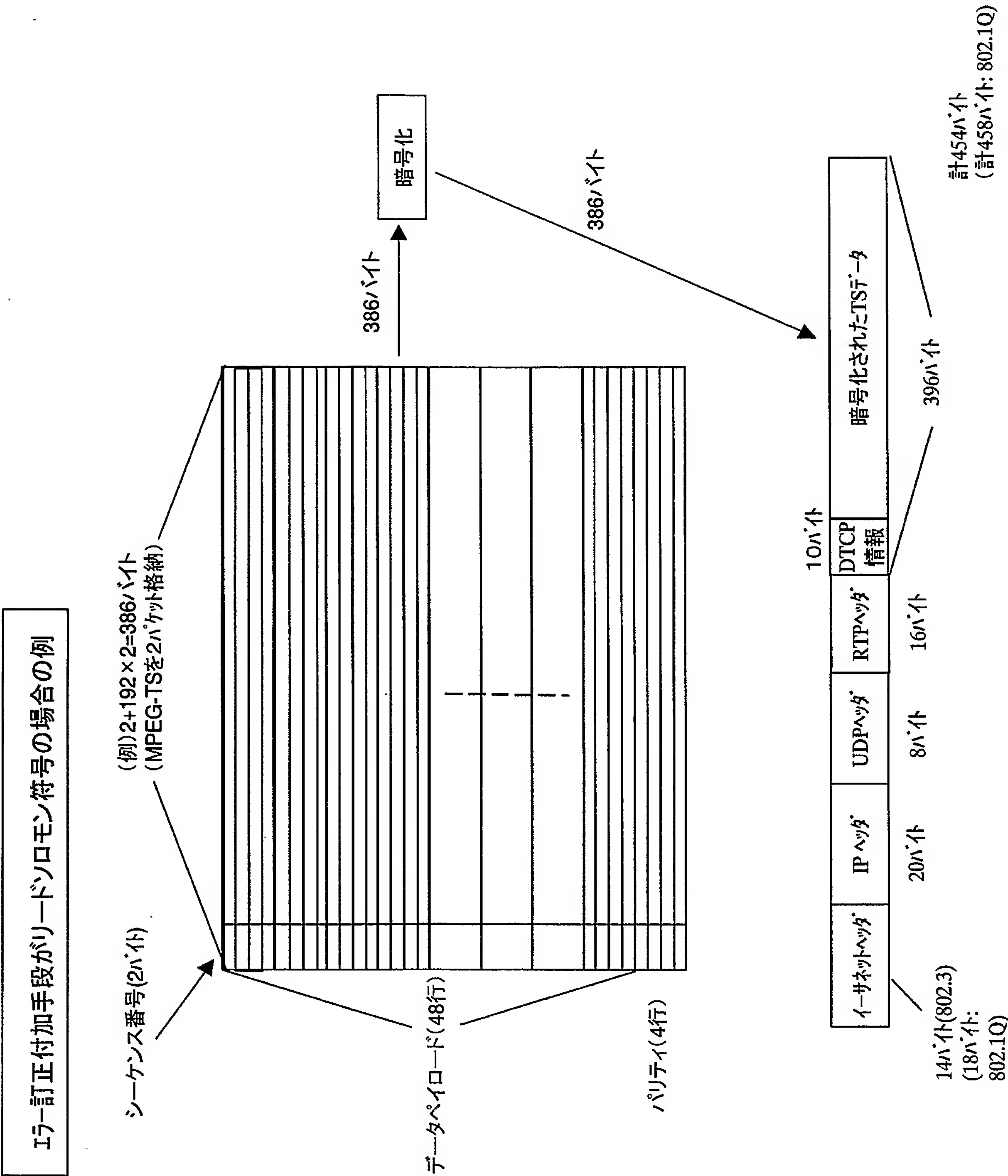


【図 15】

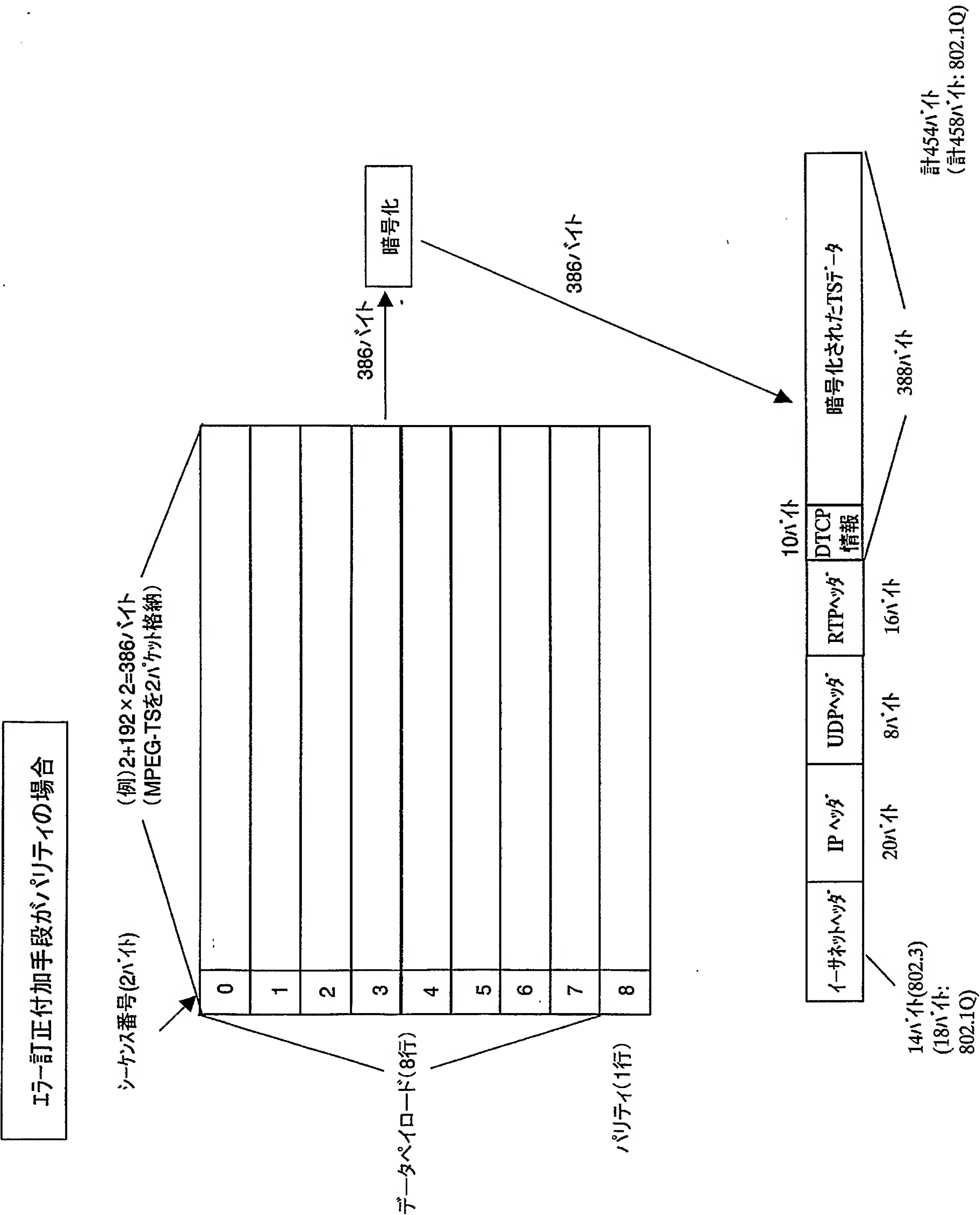


(OSIモデルによる説明)

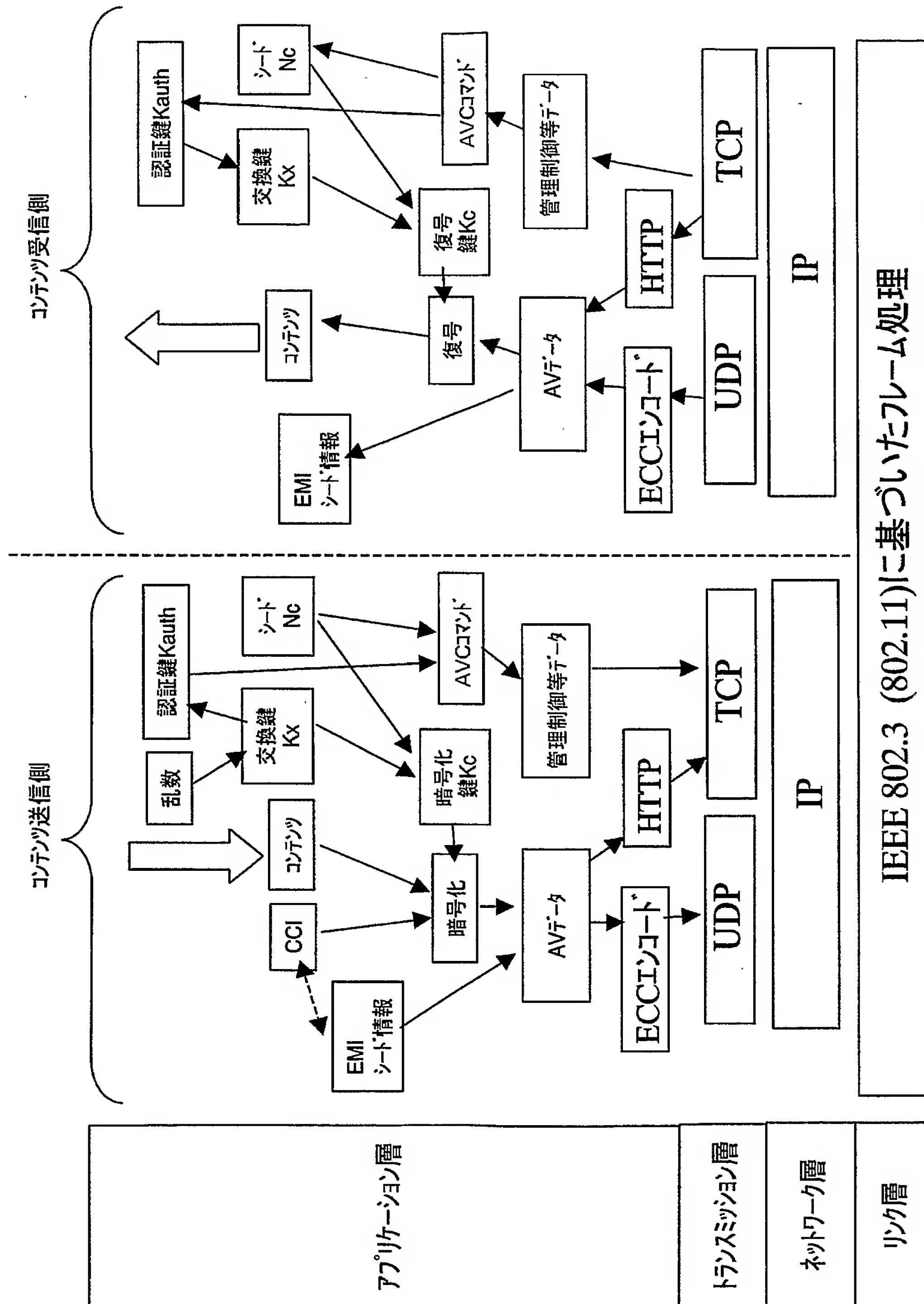
【図 1 6】



【図 1 7】

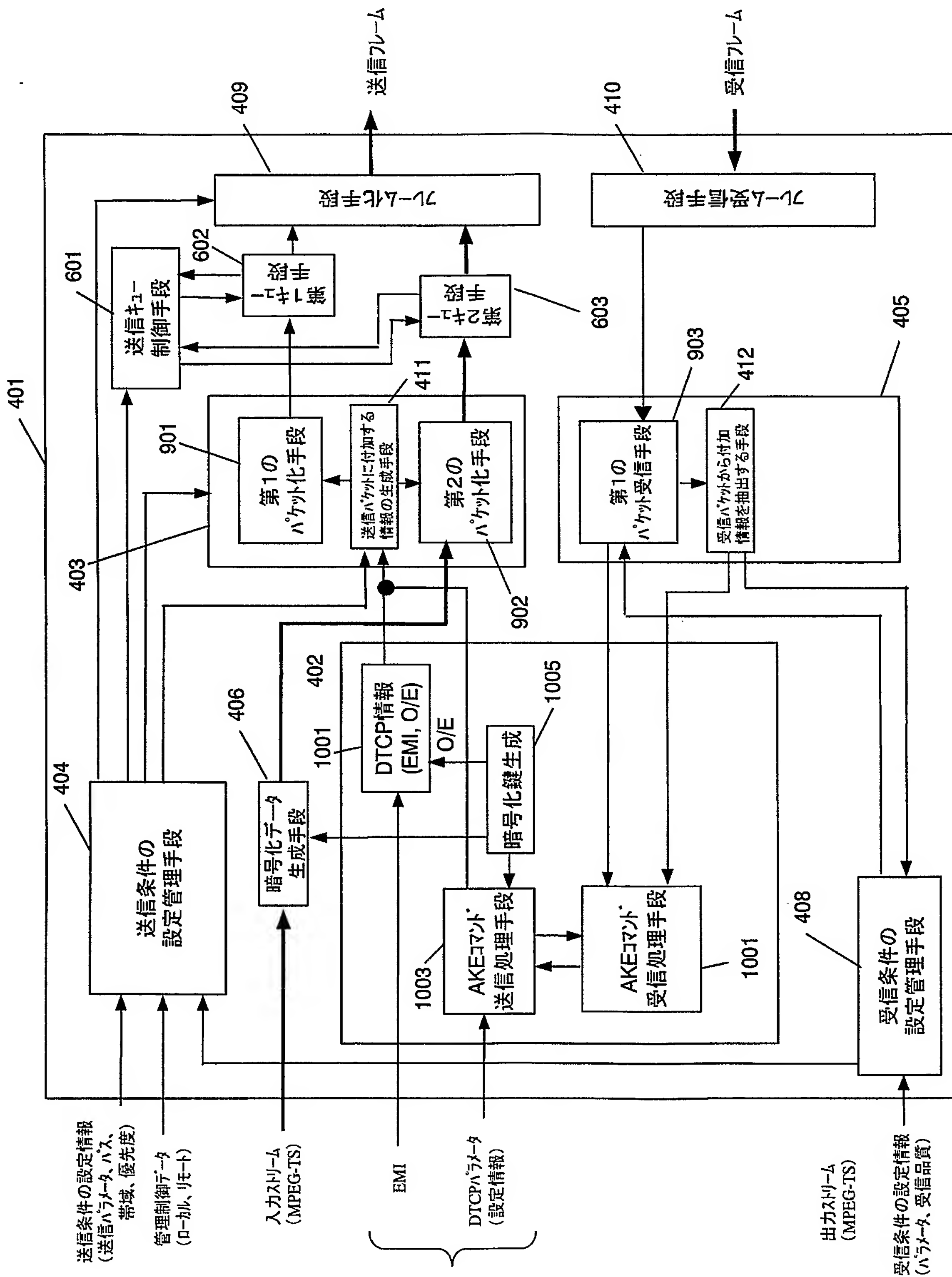


【図 18】

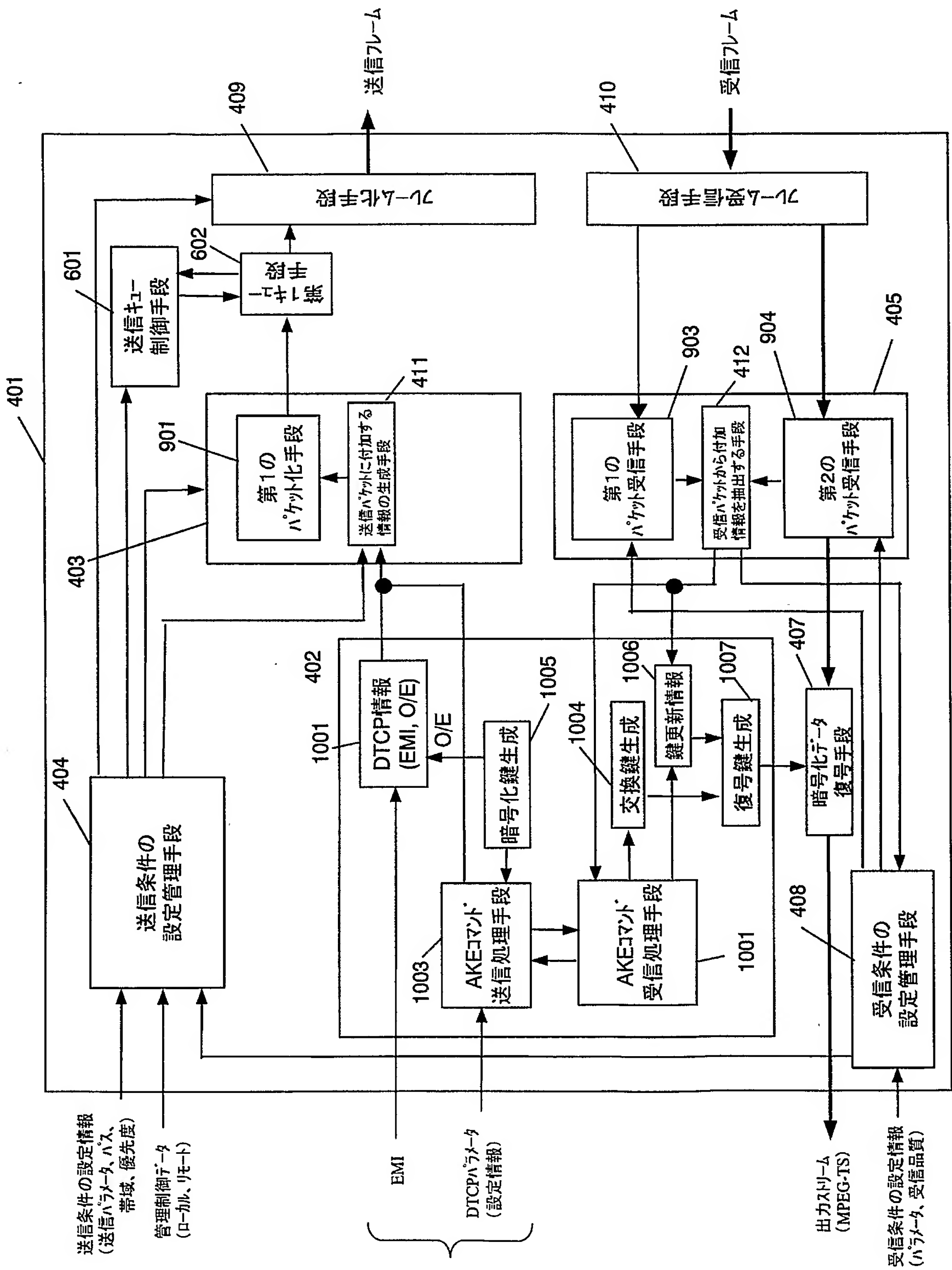


(OSIモデルによる説明)

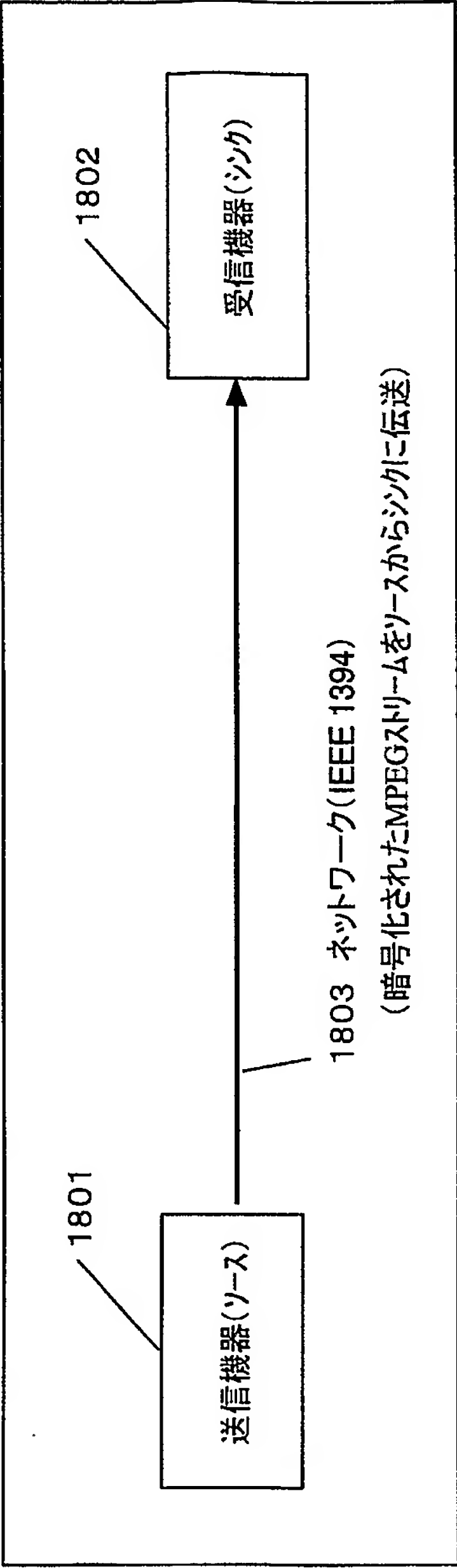
【図 19】



【図 20】



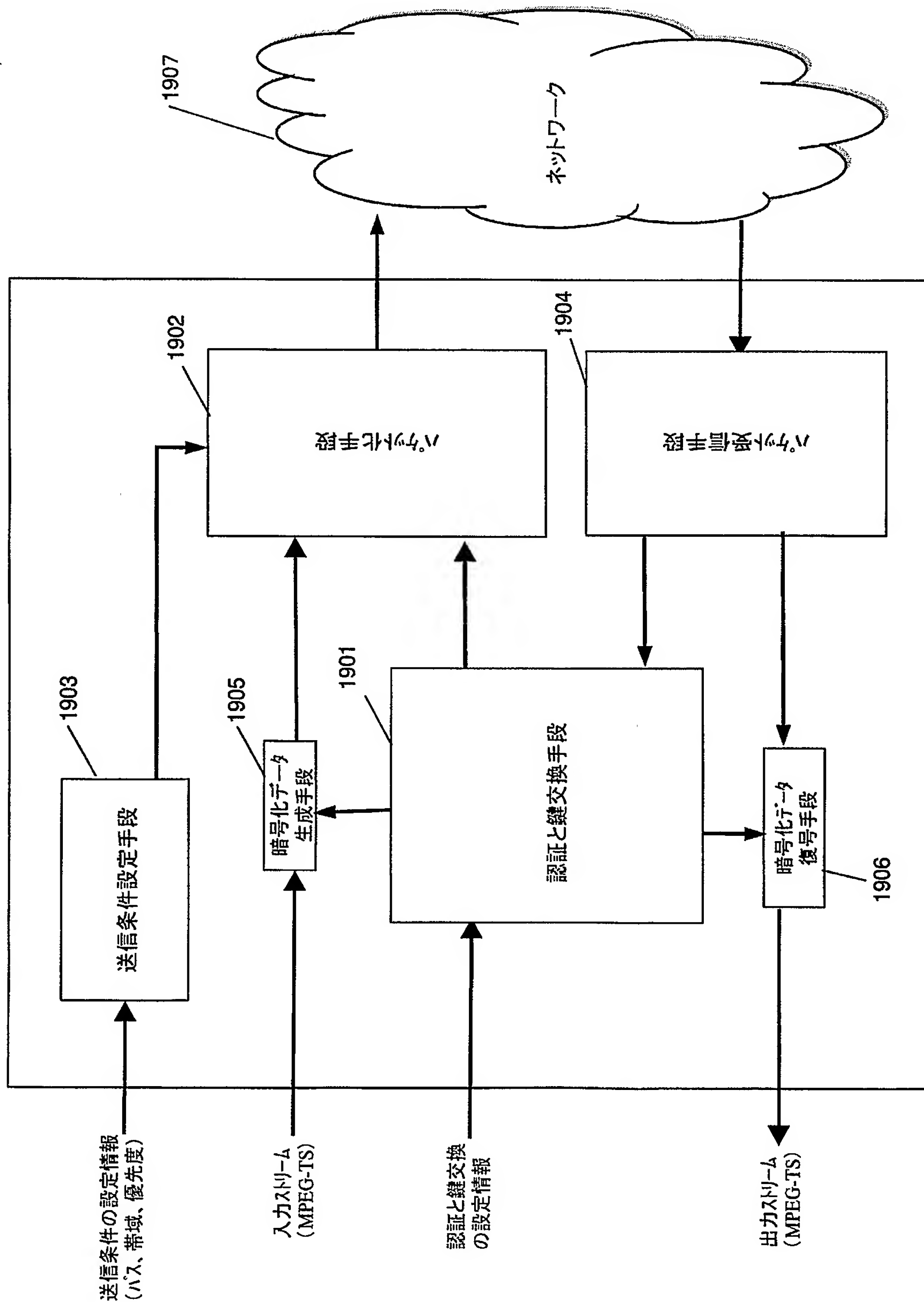
【図 2 1】



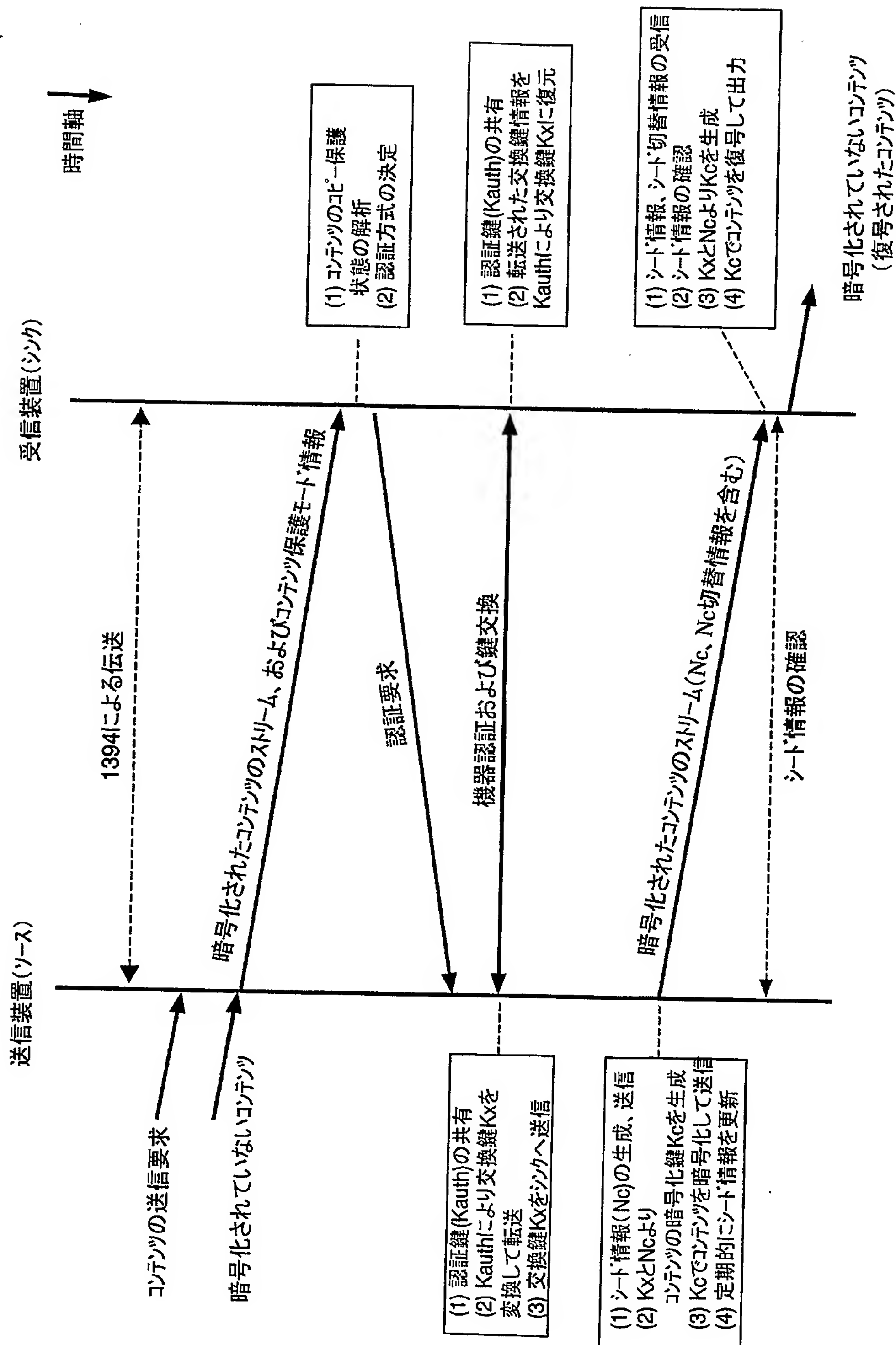
送信機器(ソース)の例	受信機器(シンク)の例	コンテンツ伝送における暗号化
DVHS	DVHS	MPEG-TSにDTCP方式 によるコンテンツ保護を実施
HDDレコーダ	HDDレコーダ	
1394搭載STB	1394搭載STB	
1394搭載デジタルTV	1394搭載デジタルTV	

IEEE 1394においてDTCPを用いたMPEGストリームの伝送

【図 22】

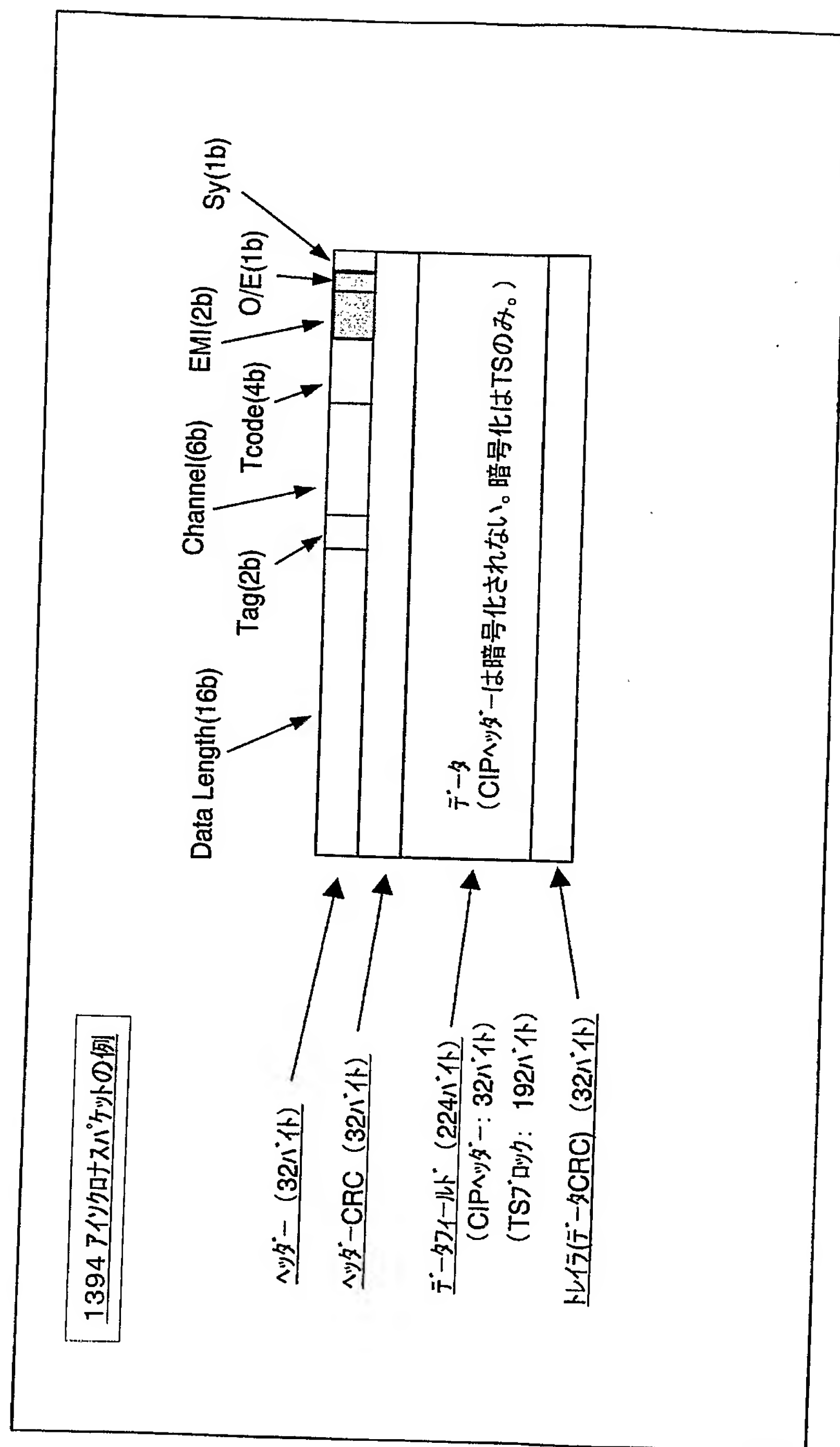


【図 23】



IEEE 1394においてDTCPを用いた暗号化ストリーム伝送手順(従来技術)

【図 2 4】



【書類名】 要約書

【要約】

【課題】 デジタル放送やDVDディスクなどの著作権保護されたMP E Gコンテンツを、そのコピー制御情報（C C I）を継承しつつ、I Pネットワークを用いてリアルタイムまたはノンリアルタイムで伝送する手段を実現する。

【解決手段】 本願発明によるパケット送信手段は、A Vデータと非A Vデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかを制御する手段とを具備する。

【選択図】 図 4

特願 2 0 0 3 - 4 1 2 9 7 9

ページ : 1/E

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社